



CCNA Exploration 4.0

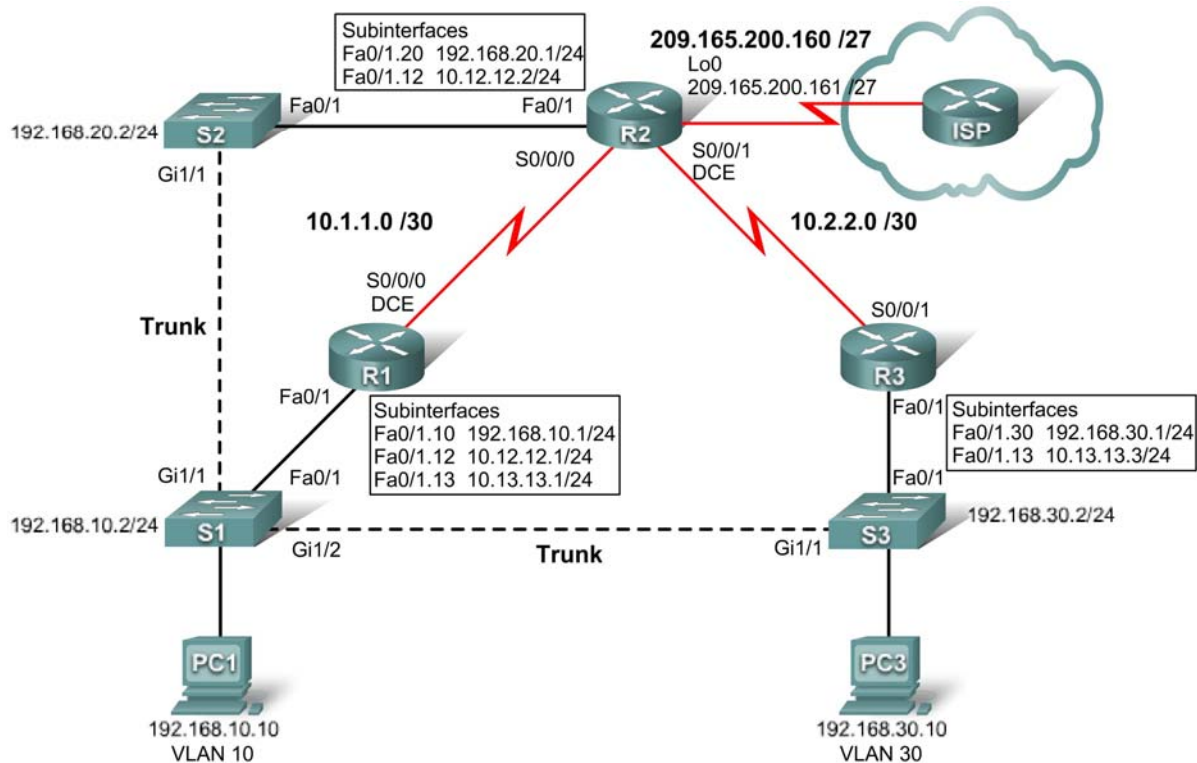
Accessing the WAN

Student Lab Manual

This document is exclusive property of Cisco Systems, Inc. Permission is granted to print and copy this document for non-commercial distribution and exclusive use by instructors in the CCNA Exploration: Accessing the WAN course as part of an official Cisco Networking Academy Program.

Lab 1.4.1: Challenge Review Lab

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1	N/A	N/A	N/A
	Fa0/1.10	192.168.10.1	255.255.255.0	N/A
	Fa0/1.12	10.12.12.1	255.255.255.0	N/A
	Fa0/1.13	10.13.13.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	Fa0/1	N/A	N/A	N/A
	Fa0/1.12	10.12.12.2	255.255.255.0	N/A
	Fa0/1.20	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	Fa0/1	N/A	N/A	N/A

	Fa0/1.13	10.13.13.3	255.255.255.0	N/A
	Fa0/1.30	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
S1	VLAN10	192.168.10.2	255.255.255.0	192.168.10.1
S2	VLAN20	192.168.20.2	255.255.255.0	192.168.20.1
S3	VLAN30	192.168.30.2	255.255.255.0	192.168.30.1
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1

Learning Objectives

To complete this lab:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Perform basic configuration tasks on a router
- Configure and activate interfaces
- Configure Spanning Tree Protocol
- Configure VTP servers and client
- Configure VLANs on the switches
- Configure RIP routing on all the routers
- Configure OSPF routing on all routers
- Configure EIGRP routing on all the routers

Scenario

In this lab, you will review basic routing and switching concepts. Try to do as much on your own as possible. Refer back to previous material when you cannot proceed on your own.

Note: Configuring three separate routing protocols—RIP, OSPF, and EIGRP—to route the same network is emphatically *not* a best practice. It should be considered a worst practice and is not something that would be done in a production network. It is done here so that you can review the major routing protocols before proceeding, and see a dramatic illustration of the concept of administrative distance.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Device Configurations.

Configure the R1, R2, and R3 routers and the S1, S2, S3 switches according to the following guidelines:

- Configure the hostname.
- Disable DNS lookup.
- Configure an EXEC mode password.

- Configure a message-of-the-day banner.
- Configure a password for console connections.
- Configure synchronous logging.
- Configure a password for vty connections.

Task 3: Configure and Activate Serial and Ethernet Addresses

Step 1: Configure interfaces on R1, R2, and R3.

Step 2: Verify IP addressing and interfaces.

Step 3: Configure the Management VLAN interface on S1, S2, and S3.

Step 4: Configure the PC1 and PC3 Ethernet interfaces.

Step 5: Test connectivity between the PCs.

Task 4: Configure STP

Step 1: Configure S1 to always be root.

Step 2: Verify that S1 is root.

Task 5: Configure VTP

Step 1: Configure S1 as the VTP server and create a domain name and password.

Step 2: Configure S2 and S3 as VTP clients as assign domain names and passwords.

Step 3: Verify the configuration.

Task 6: Configure VLANs

Step 1: Configure S1 with VLANs.

Step 2: Verify that S2 and S3 received VLAN configurations from S1.

Step 3: Assign ports to the appropriate VLANs.

Task 7: Configure RIP Routing

Step 1: Configure RIP routing on R1, R2, and R3.

Step 2: Test connectivity with ping.

Step 3: Verify the routing table.

Task 8: Configure OSPF Routing

Step 1: Configure OSPF routing on R1, R2, and R3.

Step 2: Verify that OSPF routes have replaced RIP routes because of lower administrative distance.

How are the routing decisions different now that OSPF is running?

Step 3: Verify that RIP is still running.

Task 9: Configure EIGRP Routing

Step 1: Configure EIGRP routing on R1, R2, and R3.

Step 2: Verify that EIGRP routes have replaced OSPF routes because of lower administrative distance.

Step 3: Verify that OSPF is still running.

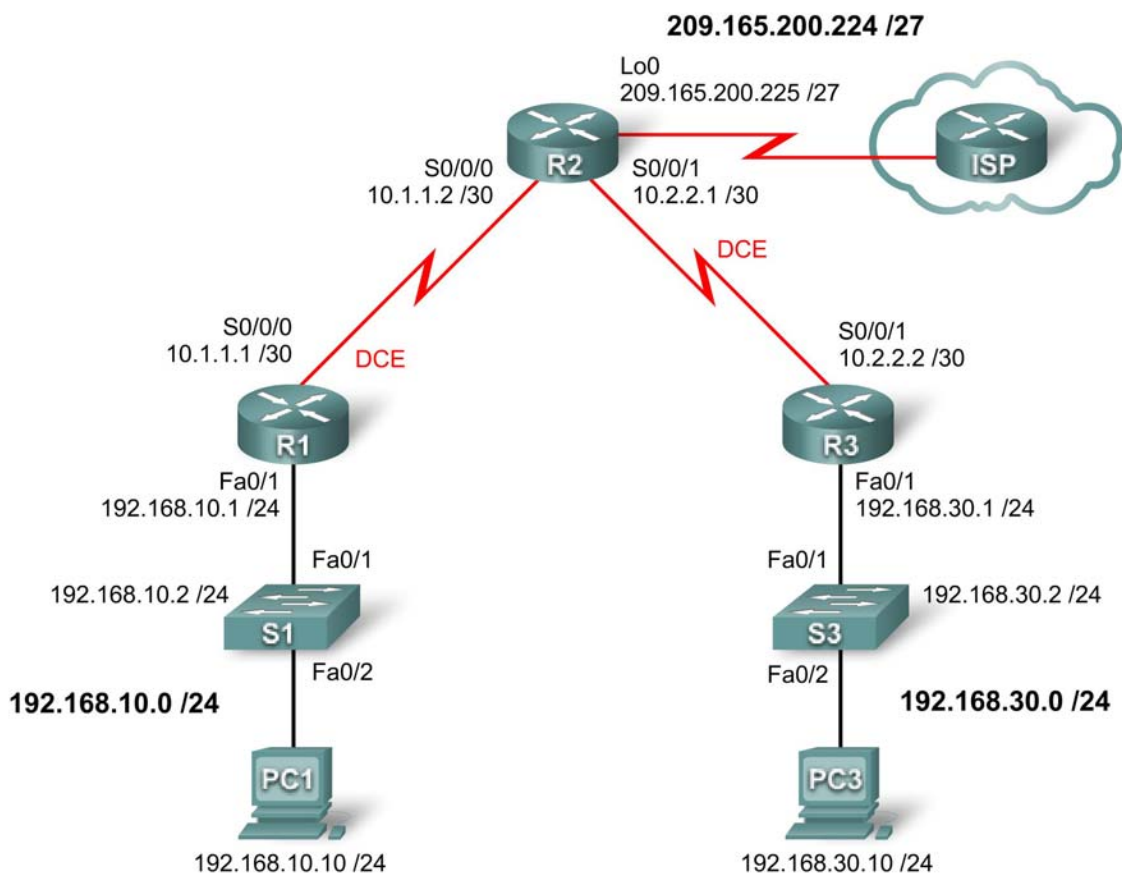
Task 10: Document the Router Configurations

Task 11: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 2.5.1: Basic PPP Configuration Lab

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1	192.168.10.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	Lo0	209.165.200.225	255.255.255.224	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	Fa0/1	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1

PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
-----	-----	---------------	---------------	--------------

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Perform basic configuration tasks on a router
- Configure and activate interfaces
- Configure OSPF routing on all routers
- Configure PPP encapsulation on all serial interfaces
- Learn about the **debug ppp negotiation** and **debug ppp packet** commands
- Learn how to change the encapsulation on the serial interfaces from PPP to HDLC
- Intentionally break and restore PPP encapsulation
- Configure PPP PAP and CHAP authentication
- Intentionally break and restore PPP PAP and CHAP authentication

Scenario

In this lab, you will learn how to configure PPP encapsulation on serial links using the network shown in the topology diagram. You will also learn how to restore serial links to their default HDLC encapsulation. Pay special attention to what the output of the router looks like when you intentionally break PPP encapsulation. This will assist you in the Troubleshooting lab associated with this chapter. Finally, you will configure PPP PAP authentication and PPP CHAP authentication.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology diagram.

Note: If you use 1700, 2500, or 2600 routers, the router outputs and interface descriptions appear differently.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configuration

Configure the R1, R2, and R3 routers according to the following guidelines:

- Configure the router hostname.
- Disable DNS lookup.
- Configure an EXEC mode password.

- Configure a message-of-the-day banner.
- Configure a password for console connections.
- Configure synchronous logging.
- Configure a password for vty connections.

Task 3: Configure and Activate Serial and Ethernet Addresses

Step 1: Configure interfaces on R1, R2, and R3.

Configure the interfaces on the R1, R2, and R3 routers with the IP addresses from the addressing table at the beginning of the lab. Be sure to include the clock rate on the serial DCE interfaces.

Step 2: Verify IP addressing and interfaces.

Use the **show ip interface brief** command to verify that the IP addressing is correct and that the interfaces are active.

When you have finished, be sure to save the running configuration to the NVRAM of the router.

Step 3: Configure the Ethernet interfaces of PC1 and PC3.

Configure the Ethernet interfaces of PC1 and PC3 with the IP addresses and default gateways from the addressing table.

Step 4: Test the configuration by pinging the default gateway from the PC.

Task 4: Configure OSPF on the Routers

If you need to review the OSPF commands, see Exploration 2, module 11.

Step 1: Enable OSPF routing on R1, R2, and R3.

Use the **router ospf** command with a process ID of 1. Be sure to advertise the networks.

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.10.0 0.0.0.255 area 0
R1(config-router)#network 10.1.1.0 0.0.0.3 area 0
*Aug 17 17:49:14.689: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from LOADING to FULL, Loading Done
R1(config-router)#
```

```
R2(config)#router ospf 1
R2(config-router)#network 10.1.1.0 0.0.0.3 area 0
*Aug 17 17:48:40.645: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-router)#network 10.2.2.0 0.0.0.3 area 0
R2(config-router)#network 209.165.200.224 0.0.0.31 area 0
R2(config-router)#
*Aug 17 17:57:44.729: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOADING to FULL, Loading Done
R2(config-router)#
```

```
R3(config)#router ospf 1
R3(config-router)#network 10.2.2.0 0.0.0.3 area 0
*Aug 17 17:58:02.017: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
```



```
Serial0/0/1 from LOADING to FULL, Loading Done
R3(config-router)#network 192.168.30.0 0.0.0.255 area 0
R3(config-router)#
```

Step 2: Verify that you have full network connectivity.

Use the **show ip route** and **ping** commands to verify connectivity.

```
R1#show ip route
```

<output omitted>

```
O    192.168.30.0/24 [110/1563] via 10.1.1.2, 00:33:56, Serial0/0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/1
    209.165.200.0/32 is subnetted, 1 subnets
O      209.165.200.225 [110/782] via 10.1.1.2, 00:33:56, Serial0/0/0
    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C      10.1.1.2/32 is directly connected, Serial0/0/0
O      10.2.2.0/30 [110/1562] via 10.1.1.2, 00:33:56, Serial0/0/0
C      10.1.1.0/30 is directly connected, Serial0/0/0
```

```
R1#ping 192.168.30.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms

R1#

```
R2#show ip route
```

<output omitted>

```
O    192.168.30.0/24 [110/782] via 10.2.2.2, 00:33:04, Serial0/0/1
O    192.168.10.0/24 [110/782] via 10.1.1.1, 00:33:04, Serial0/0/0
    209.165.200.0/27 is subnetted, 1 subnets
C      209.165.200.224 is directly connected, Loopback0
    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C      10.2.2.2/32 is directly connected, Serial0/0/1
C      10.2.2.0/30 is directly connected, Serial0/0/1
C      10.1.1.0/30 is directly connected, Serial0/0/0
C      10.1.1.1/32 is directly connected, Serial0/0/0
```

```
R2#ping 192.168.30.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms

```
R2#ping 192.168.10.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms

R2#

R3#**show ip route**

<output omitted>

```
C    192.168.30.0/24 is directly connected, FastEthernet0/1
O    192.168.10.0/24 [110/1563] via 10.2.2.1, 00:32:01, Serial0/0/1
    209.165.200.0/32 is subnetted, 1 subnets
O      209.165.200.225 [110/782] via 10.2.2.1, 00:32:01, Serial0/0/1
    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C      10.2.2.0/30 is directly connected, Serial0/0/1
O      10.1.1.0/30 [110/1562] via 10.2.2.1, 00:32:01, Serial0/0/1
C      10.2.2.1/32 is directly connected, Serial0/0/1
```

R3#**ping 209.165.200.225**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms

R3#**ping 192.168.10.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms

R3#

Task 5: Configure PPP Encapsulation on Serial Interfaces

Step 1: Use the show interface command to check whether HDLC is the default serial encapsulation.

R1#**show interface serial0/0/0**

Serial0/0/0 is up, line protocol is up

Hardware is GT96K Serial

Internet address is 10.1.1.1/30

MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation HDLC, loopback not set

<output omitted>

R2#**show interface serial 0/0/0**

Serial0/0/0 is up, line protocol is up

Hardware is GT96K Serial

Internet address is 10.1.1.2/30

MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation HDLC, loopback not set

<output omitted>

R2#**show interface serial 0/0/1**

Serial0/0/1 is up, line protocol is up

```
Hardware is GT96K Serial
Internet address is 10.2.2.1/30
MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
```

<output omitted>

```
R3#show interface serial 0/0/1
Serial0/0/1 is up, line protocol is up
Hardware is GT96K Serial
Internet address is 10.2.2.2/30
MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
```

<output omitted>

Step 2: Use debug commands on R1 and R2 to see the effects of configuring PPP.

```
R1#debug ppp negotiation
PPP protocol negotiation debugging is on
R1#debug ppp packet
PPP packet display debugging is on
R1#
```

```
R2#debug ppp negotiation
PPP protocol negotiation debugging is on
R2#debug ppp packet
PPP packet display debugging is on
R2#
```

Step 3: Change the encapsulation of the serial interfaces from HDLC to PPP.

Change the encapsulation type on the link between R1 and R2, and observe the effects. If you start to receive too much debug data, use the **undebg all** command to turn debugging off.

```
R1(config)#interface serial 0/0/0
R1(config-if)#encapsulation ppp
R1(config-if)#
*Aug 17 19:02:53.412: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or
detached
R1(config-if)#
*Aug 17 19:02:53.416: Se0/0/0 PPP: Phase is DOWN, Setup
*Aug 17 19:02:53.416: Se0/0/0 PPP: Using default call direction
*Aug 17 19:02:53.416: Se0/0/0 PPP: Treating connection as a dedicated
line
*Aug 17 19:02:53.416: Se0/0/0 PPP: Session handle[E4000001] Session
id[0]
*Aug 17 19:02:53.416: Se0/0/0 PPP: Phase is ESTABLISHING, Active Open
*Aug 17 19:02:53.424: Se0/0/0 LCP: O CONFREQ [Closed] id 1 len 10
*Aug 17 19:02:53.424: Se0/0/0 LCP: MagicNumber 0x63B994DE
(0x050663B994DE)
R1(config-if)#
*Aug 17 19:02:55.412: Se0/0/0 PPP: Outbound cdp packet dropped
*Aug 17 19:02:55.432: Se0/0/0 LCP: TIMEOUT: State REQsent
```

```
*Aug 17 19:02:55.432: Se0/0/0 LCP: O CONFREQ [REQsent] id 2 len 10
*Aug 17 19:02:55.432: Se0/0/0 LCP:      MagicNumber 0x63B994DE
(0x050663B994DE)
*Aug 17 19:02:56.024: Se0/0/0 PPP: I pkt type 0x008F, datagramsize 24
link[illegal]
*Aug 17 19:02:56.024: Se0/0/0 UNKNOWN(0x008F): Non-NCP packet,
discarding
R1(config-if)#
*Aug 17 19:02:57.252: Se0/0/0 PPP: I pkt type 0x000F, datagramsize 84
link[illegal]
*Aug 17 19:02:57.252: Se0/0/0 UNKNOWN(0x000F): Non-NCP packet,
discarding
*Aug 17 19:02:57.448: Se0/0/0 LCP: TIMEOUT: State REQsent
*Aug 17 19:02:57.448: Se0/0/0 LCP: O CONFREQ [REQsent] id 3 len 10
*Aug 17 19:02:57.448: Se0/0/0 LCP:      MagicNumber 0x63B994DE
(0x050663B994DE)
R1(config-if)#
*Aug 17 19:02:58.412: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
```

```
R2(config)#interface serial 0/0/0
R2(config-if)#encapsulation ppp
R2(config-if)#
*Aug 17 19:06:48.848: Se0/0/0 PPP: Phase is DOWN, Setup
*Aug 17 19:06:48.848: Se0/0/0 PPP: Using default call direction
*Aug 17 19:06:48.848: Se0/0/0 PPP: Treating connection as a dedicated
line
*Aug 17 19:06:48.848: Se0/0/0 PPP: Session handle[C6000001] Session
id[0]
*Aug 17 19:06:48.848: Se0/0/0 PPP: Phase is ESTABLISHING, Active Open
*Aug 17 19:06:48.856: Se0/0/0 LCP: O CONFREQ [Closed] id 1 len 10
*Aug 17 19:06:48.856: Se0/0/0 LCP:      MagicNumber 0x63BD388C
(0x050663BD388C)
*Aug 17 19:06:48.860: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14
link[ppp]
*Aug 17 19:06:48.860: Se0/0/0 LCP: I CONFACK [REQsent] id 1 len 10
R2(config-if)#
*Aug 17 19:06:48.860: Se0/0/0 LCP:      MagicNumber 0x63BD388C
(0x050663BD388C)
R2(config-if)#
*Aug 17 19:06:50.864: Se0/0/0 LCP: TIMEOUT: State ACKrcvd
*Aug 17 19:06:50.864: Se0/0/0 LCP: O CONFREQ [ACKrcvd] id 2 len 10
*Aug 17 19:06:50.864: Se0/0/0 LCP:      MagicNumber 0x63BD388C
(0x050663BD388C)
*Aug 17 19:06:50.868: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14
link[ppp]
*Aug 17 19:06:50.868: Se0/0/0 LCP: I CONFREQ [REQsent] id 61 len 10
*Aug 17 19:06:50.868: Se0/0/0 LCP:      MagicNumber 0x63BDB9A8
(0x050663BDB9A8)
*Aug 17 19:06:50.868: Se0/0/0 LCP: O CONFACK [REQsent] id 61 len 10
*Aug 17 19:06:50.868: Se0/0/0 LCP:      MagicNumber 0x63BDB9A8
(0x050663BDB9A8)
*Aug 17 19:06:50.868: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14
link[ppp]
*Aug 17 19:06:50.868: Se0/0/0 LCP: I CONFACK [ACKsent] id 2 len 10
*Aug 17 19:06:50.868: Se0/0/0 LCP:      MagicNumber 0x63BD388C
```

```
(0x050663BD388C)
*Aug 17 19:06:50.868: Se0/0/0 LCP: State is Open
*Aug 17 19:06:50.872: Se0/0/0 PPP: Phase is FORWARDING, Attempting
Forward
*Aug 17 19:06:50.872: Se0/0/0 PPP: Phase is ESTABLISHING, Finish LCP
*Aug 17 19:06:50.872: Se0/0/0 PPP: Phase is UP
*Aug 17 19:06:50.872: Se0/0/0 IPCP: O CONFREQ [Closed] id 1 len 10
*Aug 17 19:06:50.872: Se0/0/0 IPCP: Address 10.1.1.2
(0x03060A010102)
*Aug 17 19:06:50.872: Se0/0/0 CDPCP: O CONFREQ [Closed] id 1 len 4
*Aug 17 19:06:50.872: Se0/0/0 PPP: Process pending ncp packets
*Aug 17 19:06:50.876: Se0/0/0 PPP: I pkt type 0x8021, datagramsize 14
link[ip]
*Aug 17 19:06:50.876: Se0/0/0 IPCP: I CONFREQ [REQsent] id 1 len 10
*Aug 17 19:06:50.876: Se0/0/0 IPCP: Address 10.1.1.1
(0x03060A010101)
*Aug 17 19:06:50.876: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8
link[cdp]
*Aug 17 19:06:50.876: Se0/0/0 IPCP: O CONFACK [REQsent] id 1 len 10
*Aug 17 19:06:50.876: Se0/0/0 IPCP: Address 10.1.1.1
(0x03060A010101)
*Aug 17 19:06:50.876: Se0/0/0 CDPCP: I CONFREQ [REQsent] id 1 len 4
*Aug 17 19:06:50.876: Se0/0/0 CDPCP: O CONFACK [REQsent] id 1 len 4
*Aug 17 19:06:50.876: Se0/0/0 PPP: I pkt type 0x8021, datagramsize 14
link[ip]
*Aug 17 19:06:50.876: Se0/0/0 IPCP: I CONFACK [ACKse
R2(config-if)#nt] id 1 len 10
*Aug 17 19:06:50.876: Se0/0/0 IPCP: Address 10.1.1.2
(0x03060A010102)
*Aug 17 19:06:50.876: Se0/0/0 IPCP: State is Open
*Aug 17 19:06:50.876: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8
link[cdp]
*Aug 17 19:06:50.876: Se0/0/0 IPCP: Install route to 10.1.1.1
*Aug 17 19:06:50.880: Se0/0/0 CDPCP: I CONFACK [ACKsent] id 1 len 4
*Aug 17 19:06:50.880: Se0/0/0 CDPCP: State is Open
*Aug 17 19:06:50.880: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
*Aug 17 19:06:50.880: Se0/0/0 IPCP: Add link info for cef entry
10.1.1.1
*Aug 17 19:06:50.884: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80
link[ip]
*Aug 17 19:06:51.848: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
R2(config-if)#
*Aug 17 19:06:51.888: Se0/0/0 LCP-FS: I ECHOREQ [Open] id 1 len 12
magic 0x63BDB9A8
*Aug 17 19:06:51.888: Se0/0/0 LCP-FS: O ECHOREP [Open] id 1 len 12
magic 0x63BD388C

<output omitted>

*Aug 17 19:07:00.936: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from LOADING to FULL, Loading Done
```

What happens when one end of the serial link is encapsulated with PPP and the other end of the link is encapsulated with HDLC?

What steps does PPP go through when the other end of the serial link on R2 is configured with PPP encapsulation?

What happens when PPP encapsulation is configured on each end of the serial link?

Step 4: Turn off debugging.

Turn off debugging if you have not already used the **undebug all** command.

```
R1#undebug all
```

Port Statistics for unclassified packets is not turned on.

All possible debugging has been turned off

```
R1#
```

```
R2#undebug all
```

Port Statistics for unclassified packets is not turned on.

All possible debugging has been turned off

```
R2#
```

Step 5: Change the encapsulation from HDLC to PPP on both ends of the serial link between R2 and R3.

```
R2(config)#interface serial0/0/1
```

```
R2(config-if)#encapsulation ppp
```

```
R2(config-if)#
```

```
*Aug 17 20:02:08.080: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on  
Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or  
detached
```

```
R2(config-if)#
```

```
*Aug 17 20:02:13.080: %LINEPROTO-5-UPDOWN: Line protocol on Interface  
Serial0/0/1, changed state to down
```

```
R2(config-if)#
*Aug 17 20:02:58.564: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
R2(config-if)#
*Aug 17 20:03:03.644: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOADING to FULL, Loading Done
R2(config-if)#

*Aug 17 20:03:46.988: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
R3(config)#interface serial 0/0/1
R3(config-if)#encapsulation ppp
R3(config-if)#
*Aug 17 20:04:27.152: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
*Aug 17 20:04:30.952: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from LOADING to FULL, Loading Done
```

When does the line protocol on the serial link come up and the OSPF adjacency is restored?

Step 7: Verify that PPP is now the encapsulation on the serial interfaces.

```
R1#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set
```

<output omitted>

```
R2#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.1.2/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set
```

<output omitted>

```
R2#show interface serial 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.2.2.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
```



```
Encapsulation PPP, LCP Open
Open: CDPCP, IPCP, loopback not set

<output omitted>
R3#show interface serial 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.2.2.2/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

<output omitted>
```

Task 7: Break and Restore PPP Encapsulation

By intentionally breaking PPP encapsulation, you will learn about the error messages that are generated. This will help you later in the Troubleshooting lab.

Step 1: Return both serial interfaces on R2 to their default HDLC encapsulation.

```
R2(config)#interface serial 0/0/0
R2(config-if)#encapsulation hdlc
R2(config-if)#
*Aug 17 20:36:48.432: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or
detached
*Aug 17 20:36:49.432: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
R2(config-if)#
*Aug 17 20:36:51.432: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
R2(config-if)#interface serial 0/0/1
*Aug 17 20:37:14.080: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
R2(config-if)#encapsulation hdlc
R2(config-if)#
*Aug 17 20:37:17.368: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or
detached
*Aug 17 20:37:18.368: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
R2(config-if)#
*Aug 17 20:37:20.368: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
R2(config-if)#
*Aug 17 20:37:44.080: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
R2(config-if)#
```

Why is it useful to intentionally break a configuration?

Why do both serial interfaces go down, come back up, and then go back down?

Can you think of another way to change the encapsulation of a serial interface from PPP to the default HDLC encapsulation other than using the **encapsulation hdlc** command? (Hint: It has to do with the **no** command.)

Step 2: Return both serial interfaces on R2 to PPP encapsulation.

```
R2(config)#interface s0/0/0
R2(config-if)#encapsulation ppp
*Aug 17 20:53:06.612: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
R2(config-if)#interface s0/0/1
*Aug 17 20:53:10.856: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-if)#encapsulation ppp
*Aug 17 20:53:23.332: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
R2(config-if)#
*Aug 17 20:53:24.916: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOADING to FULL, Loading Done
R2(config-if)#
```

Task 8: Configure PPP Authentication

Step 1: Configure PPP PAP authentication on the serial link between R1 and R2.

```
R1(config)#username R1 password cisco
R1(config)#int s0/0/0
R1(config-if)#ppp authentication pap
R1(config-if)#
*Aug 22 18:58:57.367: %LINEPROTO-5-UPDOWN: Line protocol on Interface
```

```
Serial0/0/0, changed state to down
R1(config-if)#
*Aug 22 18:58:58.423: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or
detached
R1(config-if)#ppp pap sent-username R2 password cisco
```

What happens when PPP PAP authentication is only configured on one end of the serial link?

```
R2(config)#username R2 password cisco
R2(config)#interface Serial0/0/0
R2(config-if)#ppp authentication pap
R2(config-if)#ppp pap sent-username R1 password cisco
R2(config-if)#
*Aug 23 16:30:33.771: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
R2(config-if)#
*Aug 23 16:30:40.815: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-if)#
```

What happens when PPP PAP authentication is configured on both ends of the serial link?

Step 2: Configure PPP CHAP authentication on the serial link between R2 and R3.

In PAP authentication, the password is not encrypted. While this is certainly better than no authentication at all, it is still highly preferable to encrypt the password that is being sent across the link. CHAP encrypts the password.

```
R2(config)#username R3 password cisco
R2(config)#int s0/0/1
R2(config-if)#ppp authentication chap
R2(config-if)#
*Aug 23 18:06:00.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
R2(config-if)#
*Aug 23 18:06:01.947: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or
detached
R2(config-if)#

R3(config)#username R2 password cisco
*Aug 23 18:07:13.074: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
```

```
R3(config)#int s0/0/1
R3(config-if)#
*Aug 23 18:07:22.174: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from LOADING to FULL, Loading Done
R3(config-if)#ppp authentication chap
R3(config-if)#
```

Notice that the line protocol on interface serial 0/0/1 changes state to UP even before the interface is configured for CHAP authentication. Can you guess why this is the case?

Step 3: Review the debug output.

To better understand the CHAP process, view the output of the **debug ppp authentication** command on R2 and R3. Then shut down interface serial 0/0/1 on R2, and issue the **no shutdown** command on interface serial 0/0/1 on R2.

```
R2#debug ppp authentication
PPP authentication debugging is on
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int s0/0/1
R2(config-if)#shutdown
R2(config-if)#
*Aug 23 18:19:21.059: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or
detached
R2(config-if)#
*Aug 23 18:19:23.059: %LINK-5-CHANGED: Interface Serial0/0/1, changed
state to administratively down
*Aug 23 18:19:24.059: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
R2(config-if)#no shutdown

*Aug 23 18:19:55.059: Se0/0/1 PPP: Using default call direction
*Aug 23 18:19:55.059: Se0/0/1 PPP: Treating connection as a dedicated
line
*Aug 23 18:19:55.059: Se0/0/1 PPP: Session handle[5B000005] Session
id[49]
*Aug 23 18:19:55.059: Se0/0/1 PPP: Authorization required
*Aug 23 18:19:55.063: %LINK-3-UPDOWN: Interface Serial0/0/1, changed
state to up
*Aug 23 18:19:55.063: Se0/0/1 CHAP: O CHALLENGE id 48 len 23 from "R2"
*Aug 23 18:19:55.067: Se0/0/1 CHAP: I CHALLENGE id 2 len 23 from "R3"
*Aug 23 18:19:55.067: Se0/0/1 CHAP: Using hostname from unknown source
*Aug 23 18:19:55.067: Se0/0/1 CHAP: Using password from AAA
*Aug 23 18:19:55.067: Se0/0/1 CHAP: O RESPONSE id 2 len 23 from "R2"
*Aug 23 18:19:55.071: Se0/0/1 CHAP: I RESPONSE id 48 len 23 from "R3"
```

```
*Aug 23 18:19:55.071: Se0/0/1 PPP: Sent CHAP LOGIN Request
*Aug 23 18:19:55.071: Se0/0/1 PPP: Received LOGIN Response PASS
*Aug 23 18:19:55.071: Se0/0/1 PPP: Sent LCP AUTHOR Request
*Aug 23 18:19:55.075: Se0/0/1 PPP: Sent IPCP AUTHOR Request
*Aug 23 18:19:55.075: Se0/0/1 LCP: Received AAA AUTHOR Response PASS
*Aug 23 18:19:55.075: Se0/0/1 IPCP: Received AAA AUTHOR Response PASS
*Aug 23 18:19:55.075: Se0/0/1 CHAP: O SUCCESS id 48 len 4
*Aug 23 18:19:55.075: Se0/0/1 CHAP: I SUCCESS id 2 len 4
*Aug 23 18:19:55.075: Se0/0/1 PPP: Sent CDPCP AUTHOR Request
*Aug 23 18:19:55.075: Se0/0/1 CDPCP: Received AAA AUTHOR Response PASS
*Aug 23 18:19:55.079: Se0/0/1 PPP: Sent IPCP AUTHOR Request
*Aug 23 18:19:56.075: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
R2(config-if)#
*Aug 23 18:20:05.135: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOADING to FULL, Loading Done
```

R3#debug ppp authentication

PPP authentication debugging is on

R3#

```
*Aug 23 18:19:04.494: %LINK-3-UPDOWN: Interface Serial0/0/1, changed
state to down
```

R3#

```
*Aug 23 18:19:04.494: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or
detached
```

```
*Aug 23 18:19:05.494: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
```

R3#

```
*Aug 23 18:19:36.494: %LINK-3-UPDOWN: Interface Serial0/0/1, changed
state to up
```

```
*Aug 23 18:19:36.494: Se0/0/1 PPP: Using default call direction
```

```
*Aug 23 18:19:36.494: Se0/0/1 PPP: Treating connection as a dedicated
line
```

```
*Aug 23 18:19:36.494: Se0/0/1 PPP: Session handle[3C000034] Session
id[52]
```

```
*Aug 23 18:19:36.494: Se0/0/1 PPP: Authorization required
```

```
*Aug 23 18:19:36.498: Se0/0/1 CHAP: O CHALLENGE id 2 len 23 from "R3"
```

```
*Aug 23 18:19:36.502: Se0/0/1 CHAP: I CHALLENGE id 48 len 23 from "R2"
```

```
*Aug 23 18:19:36.502: Se0/0/1 CHAP: Using hostname from unknown source
```

```
*Aug 23 18:19:36.506: Se0/0/1 CHAP: Using password from AAA
```

```
*Aug 23 18:19:36.506: Se0/0/1 CHAP: O RESPONSE id 48 len 23 from "R3"
```

```
*Aug 23 18:19:36.506: Se0/0/1 CHAP: I RESPONSE id 2 len 23 from "R2"
```

R3#

```
*Aug 23 18:19:36.506: Se0/0/1 PPP: Sent CHAP LOGIN Request
```

```
*Aug 23 18:19:36.506: Se0/0/1 PPP: Received LOGIN Response PASS
```

```
*Aug 23 18:19:36.510: Se0/0/1 PPP: Sent LCP AUTHOR Request
```

```
*Aug 23 18:19:36.510: Se0/0/1 PPP: Sent IPCP AUTHOR Request
```

```
*Aug 23 18:19:36.510: Se0/0/1 LCP: Received AAA AUTHOR Response PASS
```

```
*Aug 23 18:19:36.510: Se0/0/1 IPCP: Received AAA AUTHOR Response PASS
```

```
*Aug 23 18:19:36.510: Se0/0/1 CHAP: O SUCCESS id 2 len 4
```

```
*Aug 23 18:19:36.510: Se0/0/1 CHAP: I SUCCESS id 48 len 4
```

```
*Aug 23 18:19:36.514: Se0/0/1 PPP: Sent CDPCP AUTHOR Request
```

```
*Aug 23 18:19:36.514: Se0/0/1 PPP: Sent IPCP AUTHOR Request
```

```
*Aug 23 18:19:36.514: Se0/0/1 CDPCP: Received AAA AUTHOR Response PASS
```

R3#

```
*Aug 23 18:19:37.510: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
R3#
*Aug 23 18:19:46.570: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from LOADING to FULL, Loading Done
R3#
```

Task 9: Intentionally Break and Restore PPP CHAP Authentication

Step 1: Break PPP CHAP authentication.

On the serial link between R2 and R3, change the authentication protocol on interface serial 0/0/1 to PAP.

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int s0/0/1
R2(config-if)#ppp authentication pap
R2(config-if)#^Z
R2#
*Aug 24 15:45:47.039: %SYS-5-CONFIG_I: Configured from console by
console
R2#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R2#reload
```

Does changing the authentication protocol to PAP on interface serial 0/0/1 break authentication between R2 and R3?

Step 2: Restore PPP CHAP authentication on the serial link.

Notice that it is not necessary to reload the router for this change to take effect.

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int s0/0/1
R2(config-if)#ppp authentication chap
R2(config-if)#
*Aug 24 15:50:00.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
R2(config-if)#
*Aug 24 15:50:07.467: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOADING to FULL, Loading Done
R2(config-if)#
```

Step 3: Intentionally Break PPP CHAP authentication by changing the password on R3.

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R3(config)#username R2 password ciisco
R3(config)#^Z
R3#
*Aug 24 15:54:17.215: %SYS-5-CONFIG_I: Configured from console by
console
R3#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R3#reload
```

After reloading, what is the status of the line protocol on serial 0/0/1?

Step 4: Restore PPP CHAP authentication by changing the password on R3.

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#username R2 password cisco
R3(config)#
*Aug 24 16:11:10.679: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
R3(config)#
*Aug 24 16:11:19.739: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from LOADING to FULL, Loading Done
R3(config)#
```

Task 10: Document the Router Configurations

On each router, issue the **show run** command and capture the configurations.

```
R1#show run
!<output omitted>
!
hostname R1
!
!
enable secret class
!
!
!
no ip domain lookup
!
username R1 password 0 cisco
!
!
!
interface FastEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 no shutdown
!
!
```



```
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 encapsulation ppp
 clockrate 64000
 ppp authentication pap
 ppp pap sent-username R2 password 0 cisco
 no shutdown
!
!
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
!
!
banner motd ^CCUnauthorized access strictly prohibited and prosecuted
to the full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end

R2#show run
!<output omitted>

!
hostname R2
!
!
enable secret class
!
!
no ip domain lookup
!
username R3 password 0 cisco
username R2 password 0 cisco
!
!
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
!
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 encapsulation ppp
 ppp authentication pap
```

```
ppp pap sent-username R1 password 0 cisco
no shutdown
!
interface Serial0/0/1
ip address 10.2.2.1 255.255.255.252
encapsulation ppp
clockrate 64000
ppp authentication chap
no shutdown
!
!
router ospf 1
network 10.1.1.0 0.0.0.3 area 0
network 10.2.2.0 0.0.0.3 area 0
network 209.165.200.224 0.0.0.31 area 0
!
!
banner motd ^CUnauthorized access strictly prohibited and prosecuted to
the full extent of the law^C
!
line con 0
exec-timeout 0 0
password cisco
logging synchronous
login
line aux 0
line vty 0 4
password cisco
login
!
end
```

R3#show run

!<output omitted>

```
!
hostname R3
!
!
enable secret class
!
!
!
no ip domain lookup
!
username R2 password 0 cisco
!
!
!
interface FastEthernet0/1
ip address 192.168.30.1 255.255.255.0
no shutdown
!
!
interface Serial0/0/1
ip address 10.2.2.2 255.255.255.252
```

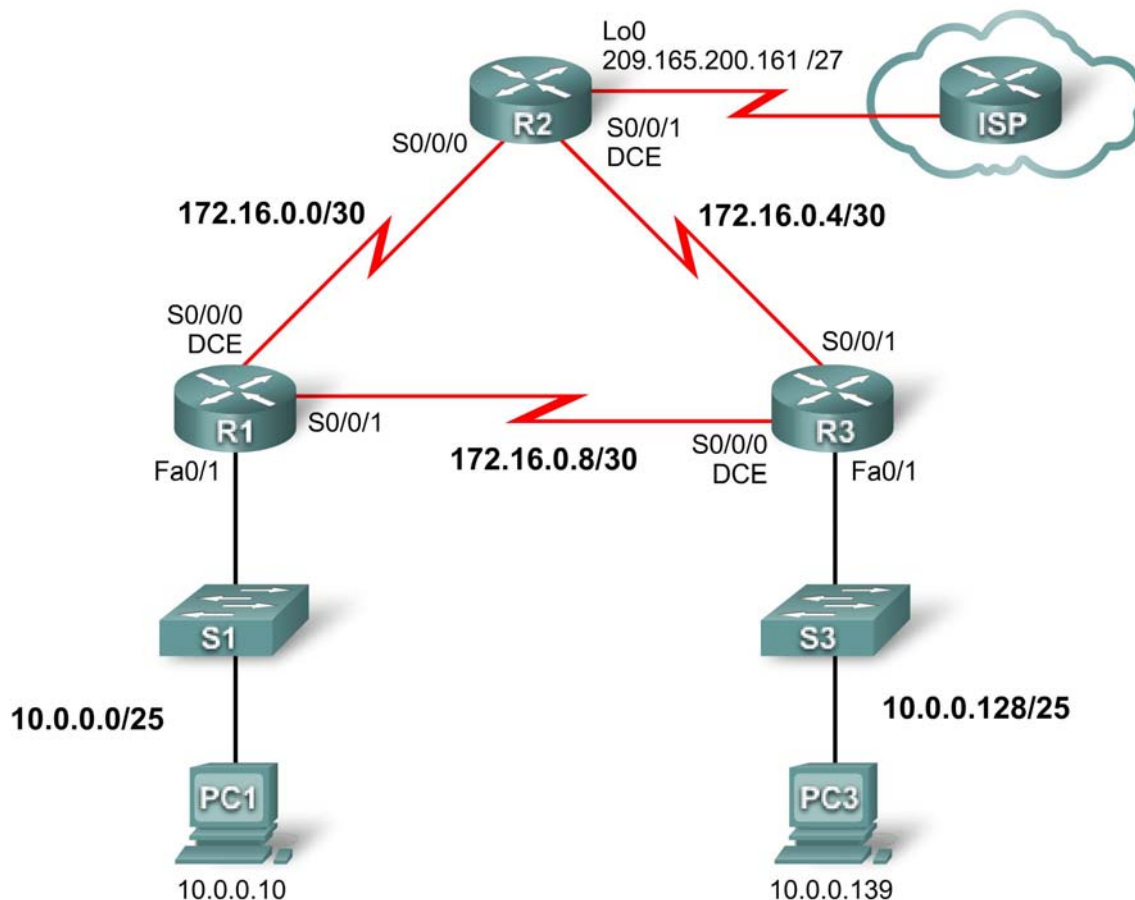
```
encapsulation ppp
ppp authentication chap
no shutdown
!
router ospf 1
 network 10.2.2.0 0.0.0.3 area 0
 network 192.168.30.0 0.0.0.255 area 0
!
!
banner motd ^CUnauthorized access strictly prohibited and prosecuted to
the full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Task 11: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks, such as the school LAN or the Internet, reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 2.5.2: Challenge PPP Configuration

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1	10.0.0.1	255.255.255.128	N/A
	S0/0/0	172.16.0.1	255.255.255.252	N/A
	S0/0/1	172.16.0.9	255.255.255.252	N/A
R2	Lo0	209.165.200.161	255.255.255.224	N/A
	S0/0/0	172.16.0.2	255.255.255.252	N/A
	S0/0/1	172.16.0.5	255.255.255.252	N/A
R3	Fa0/1	10.0.0.129	255.255.255.128	N/A

	S0/0/0	172.16.0.10	255.255.255.252	N/A
	S0/0/1	172.16.0.6	255.255.255.252	N/A
PC1	NIC	10.0.0.10	255.255.255.128	10.0.0.1
PC3	NIC	10.0.0.139	255.255.255.128	10.0.0.129

Learning Objectives

To complete this lab:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Perform basic configuration tasks on a router
- Configure and activate interfaces
- Configure OSPF routing on all routers
- Configure PPP encapsulation on all serial interfaces
- Change the encapsulation on the serial interfaces from PPP to HDLC
- Intentionally break and restore PPP encapsulation
- Configure PPP CHAP authentication
- Intentionally break and restore PPP CHAP authentication

Scenario

In this lab, you will learn how to configure PPP encapsulation on serial links using the network shown in the topology diagram. You will also configure PPP CHAP authentication. If you need assistance, refer back to the Basic PPP Configuration lab, but try to do as much on your own as possible.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configuration

Configure the R1, R2, and R3 routers according to the following guidelines:

- Configure the router hostname.
- Disable DNS lookup.
- Configure an EXEC mode password.
- Configure a message-of-the-day banner.
- Configure a password for console connections.
- Configure synchronous logging.
- Configure a password for vty connections.

Task 3: Configure and Activate Serial and Ethernet Addresses

Step 1: Configure interfaces on R1, R2, and R3.

Step 2: Verify IP addressing and interfaces.

Step 3: Configure the Ethernet interfaces of PC1 and PC3.

Step 4: Test connectivity between the PCs.

Task 4: Configure OSPF on Routers

Step 1: Enable OSPF routing on the routers.

Step 2: Verify that you have full network connectivity.

Task 5: Configure PPP Encapsulation on Serial Interfaces

Step 1: Configure PPP on the serial interfaces of all three routers.

Step 2: Verify that all serial interfaces are using PPP encapsulation.

Task 6: Intentionally Break and Restore PPP Encapsulation

Step 1: Choose a way to break PPP encapsulation on the network.

Step 2: Restore full connectivity to your network.

Step 3: Verify full connectivity to your network.

Task 7: Configure PPP CHAP Authentication

Step 1: Configure PPP CHAP authentication on all serial links.

Step 2: Verify PPP CHAP authentication on all serial links.

Task 8: Intentionally Break and Restore PPP CHAP Authentication

Step 1: Choose a way to break PPP CHAP authentication on one or more serial links.

Step 2: Verify that PPP CHAP authentication is broken.

Step 3: Restore PPP CHAP authentication on all serial links.

Step 4: Verify PPP CHAP authentication on all serial links.

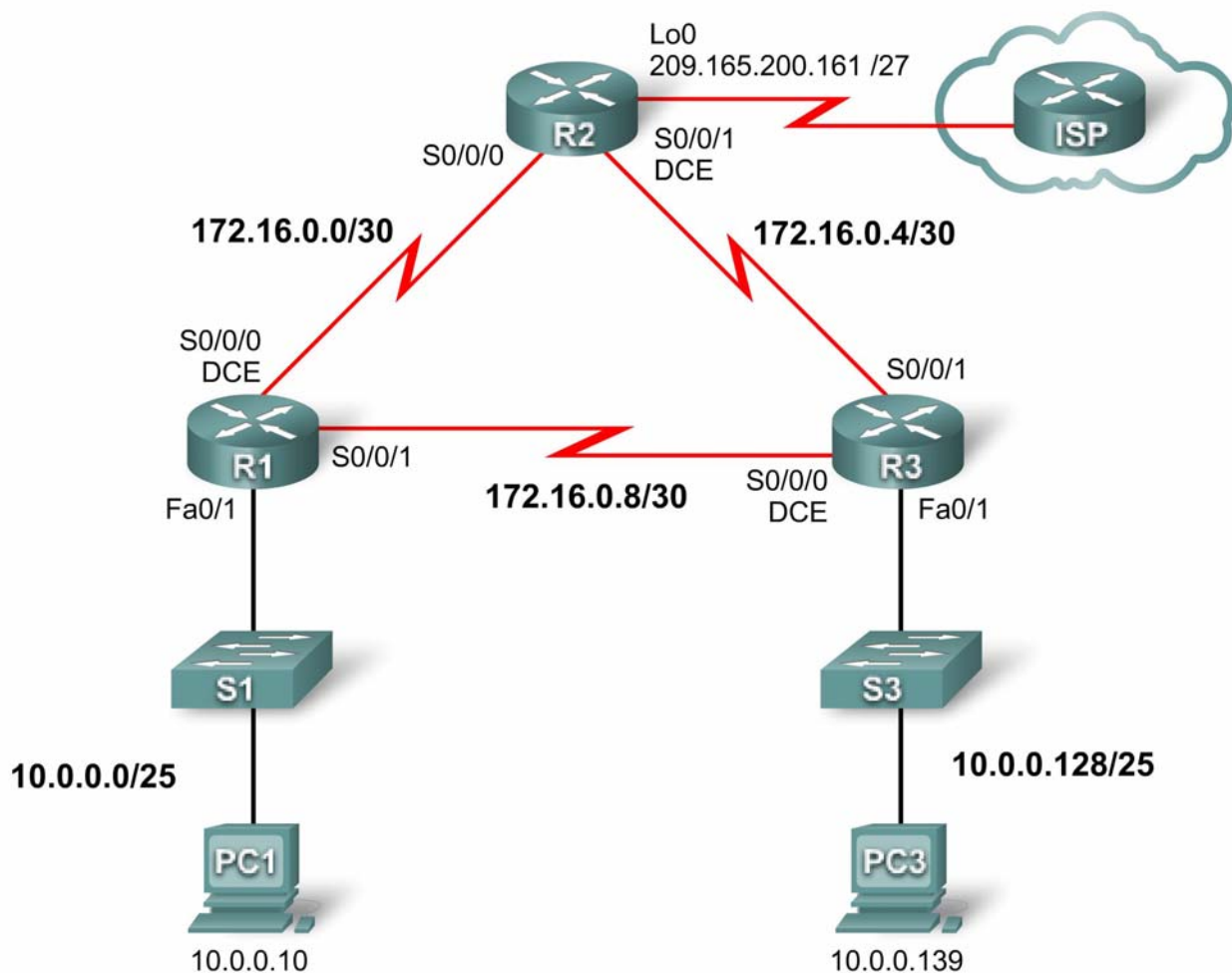
Task 9: Document the Router Configurations

Task 10: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks, such as the school LAN or the Internet, reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 2.5.3: Troubleshooting PPP Configuration

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1	10.0.0.1	255.255.255.128	N/A
	S0/0/0	172.16.0.1	255.255.255.252	N/A
	S0/0/1	172.16.0.9	255.255.255.252	N/A
R2	Lo0	209.165.200.161	255.255.255.224	N/A
	S0/0/0	172.16.0.2	255.255.255.252	N/A
	S0/0/1	172.16.0.5	255.255.255.252	N/A
R3	Fa0/1	10.0.0.129	255.255.255.128	N/A

	S0/0/0	172.16.0.10	255.255.255.252	N/A
	S0/0/1	172.16.0.6	255.255.255.252	N/A
PC1	NIC	10.0.0.10	255.255.255.128	10.0.0.1
PC3	NIC	10.0.0.139	255.255.255.128	10.0.0.129

Learning Objectives

To complete this lab:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Load routers with scripts
- Find and correct network errors
- Document the corrected network

Scenario

The routers at your company were configured by an inexperienced network engineer. Several errors in the configuration have resulted in connectivity issues. Your boss has asked you to troubleshoot and correct the configuration errors and document your work. Using your knowledge of PPP and standard testing methods, find and correct the errors. Make sure that all of the serial links use PPP CHAP authentication, and that all of the networks are reachable.

Task 1: Load Routers with the Supplied Scripts

R1

```
enable
configure terminal
!
hostname R1
!
!
enable secret class
!
!
!
no ip domain lookup
!
username R2 password 0 cisco
!
!
!
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.255.128
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 duplex auto
```

```

    speed auto
    !
interface Serial0/0/0
    ip address 172.16.0.1 255.255.255.248
    no fair-queue
    clockrate 64000
    !
interface Serial0/0/1
    ip address 172.16.0.9 255.255.255.252
    encapsulation ppp
    ppp authentication pap
    !
router ospf 1
    log-adjacency-changes
    network 10.0.0.0 0.0.0.127 area 0
    network 172.16.0.4 0.0.0.3 area 0
    network 172.16.0.8 0.0.0.3 area 0
    !
ip classless
    !
ip http server
    !
    !
control-plane
    !
banner motd ^CUnauthorized access strictly prohibited and prosecuted to the
full extent of the law^C
    !
line con 0
    exec-timeout 0 0
    password cisco
    logging synchronous
    login
line aux 0
line vty 0 4
    password cisco
    login
    !
end

```

R2

```

enable
configure terminal
    !
hostname R2
    !
    !
enable secret class
    !
    !
no ip domain lookup
    !
username R11 password 0 cisco
username R3 password 0 class
    !
    !

```

```

!
interface Loopback0
!
interface FastEthernet0/0
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 209.165.200.161 255.255.255.224
  shutdown
  duplex auto
  speed auto
!
interface Serial0/0/0
  ip address 172.16.0.2 255.255.255.252
  encapsulation ppp
  no fair-queue
  ppp authentication chap
!
interface Serial0/0/1
  ip address 172.16.0.5 255.255.255.252
!
router ospf 1
  log-adjacency-changes
  network 172.16.0.0 0.0.0.3 area 0
  network 172.16.0.4 0.0.0.3 area 0
  network 209.165.200.128 0.0.0.31 area 0
!
ip classless
!
ip http server
!
!
control-plane
!
banner motd ^CUnauthorized access strictly prohibited and prosecuted to the
full extent of the law^C
!
line con 0
  exec-timeout 0 0
  password cisco
  logging synchronous
  login
line aux 0
line vty 0 4
  password cisco
  login
!
end

```

R3

```

enable
configure terminal
!

```

```

hostname R3
!
!
enable secret class
!
!
no ip domain lookup
!
username R1 password 0 cisco
username R3 password 0 ciscoco
!
!
interface FastEthernet0/0
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 10.0.0.129 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
  ip address 172.16.0.10 255.255.255.252
  no fair-queue
  clockrate 64000
!
interface Serial0/0/1
  encapsulation ppp
  ppp authentication pap
!
router ospf 1
  log-adjacency-changes
  network 10.0.0.128 0.0.0.127 area 0
  network 192.16.0.4 0.0.0.3 area 0
  network 192.16.0.8 0.0.0.3 area 0
!
ip classless
!
ip http server
!
!
control-plane
!
banner motd ^CUnauthorized access strictly prohibited and prosecuted to the
full extent of the law^C
!
line con 0
  exec-timeout 0 0
  password cisco
  logging synchronous
  login
line aux 0
line vty 0 4
  password cisco
  login

```

```
!  
end
```

Task 2: Find and Correct Network Errors

Task 3: Document the Corrected Network

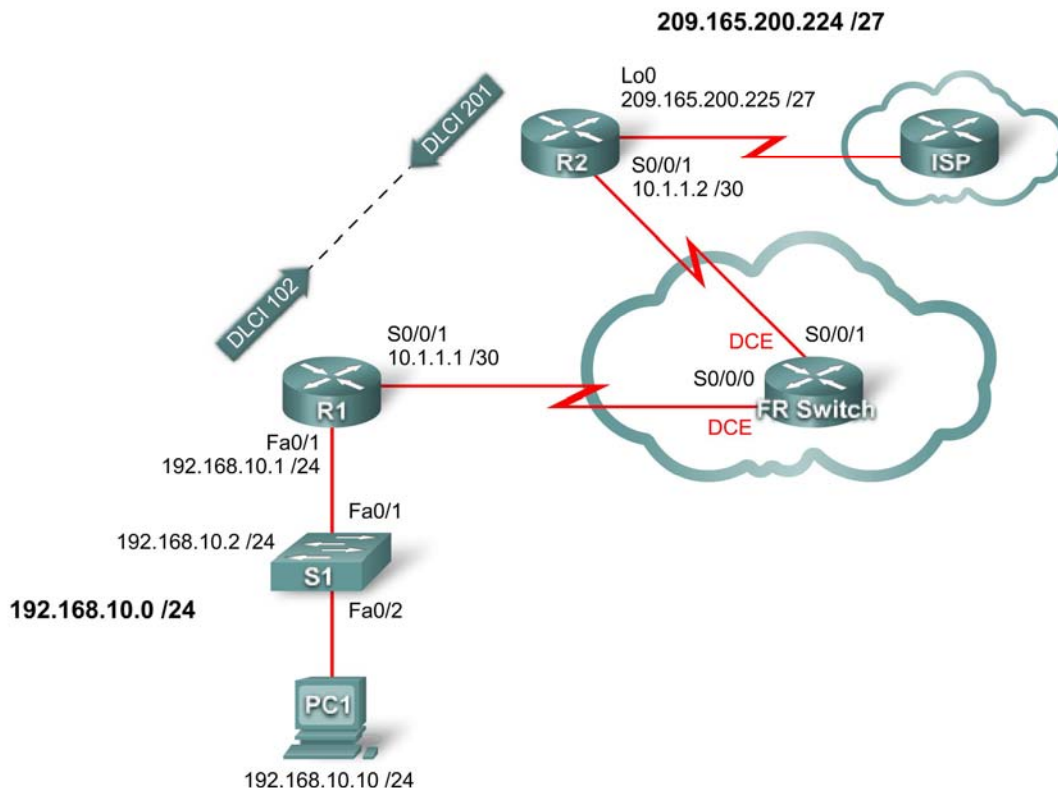
Now that you have corrected all errors and tested connectivity throughout the network, document the final configuration for each device.

Task 4: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks, such as the school LAN or the Internet, reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 3.5.1: Basic Frame Relay

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.10.1	255.255.255.0	N/A
	S0/0/1	10.1.1.1	255.255.255.252	N/A
R2	S0/0/1	10.1.1.2	255.255.255.252	N/A
	Lo 0	209.165.200.225	255.255.255.224	N/A
S1	VLAN1	192.168.10.2	255.255.255.0	192.168.10.1
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state

- Perform basic configuration tasks on a router
- Configure and activate interfaces
- Configure EIGRP routing on all routers
- Configure Frame Relay encapsulation on all serial interfaces
- Configure a router as a Frame Relay switch
- Understand the output of the **show frame-relay** commands
- Learn the effects of the **debug frame-relay lmi** command
- Intentionally break and restore a Frame Relay link
- Change the Frame Relay encapsulation type from the Cisco default to IETF
- Change the Frame Relay LMI type from Cisco to ANSI
- Configure a Frame Relay subinterface

Scenario

In this lab, you will learn how to configure Frame Relay encapsulation on serial links using the network shown in the topology diagram. You will also learn how to configure a router as a Frame Relay switch. There are both Cisco standards and Open standards that apply to Frame Relay. You will learn both. Pay special attention in the lab section in which you intentionally break the Frame Relay configurations. This will help you in the Troubleshooting lab associated with this chapter.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology. The Frame Relay labs, unlike any of the other labs in Exploration 4, have two DCE links on the same router. Be sure to change your cabling to reflect the topology diagram.

Note: If you use 1700, 2500, or 2600 routers, the router output and interface descriptions appear differently.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configuration

Configure the R1 and R2 routers and the S1 switch according to the following guidelines:

- Configure the router hostname.
 - Disable DNS lookup.
 - Configure an EXEC mode password.
 - Configure a message-of-the-day banner.
 - Configure a password for console connections.
 - Configure a password for vty connections.
 - Configure IP addresses on R1 and R2
- Important: Leave serial interfaces shut down.
- Enable EIGRP AS 1 on R1 and R2 for all networks.

```
enable
configure terminal
no ip domain-lookup
enable secret class
banner motd ^CUnauthorized access strictly prohibited, violators
will be prosecuted to the full extent of the law^C
!
!
!
line console 0
logging synchronous
password cisco
login
!
line vty 0 4
password cisco
login
end
copy running-config startup-config
```

!R1

```
interface serial 0/0/1
ip address 10.1.1.1 255.255.255.252
shutdown
```

!The serial interfaces should remain shutdown until the Frame Relay
!switch is configured

```
interface fastethernet 0/0
ip address 192.168.10.1 255.255.255.0
no shutdown
router eigrp 1
no auto-summary
network 10.0.0.0
network 192.168.10.0
!
```

!R2

```
interface serial 0/0/1
ip address 10.1.1.2 255.255.255.252
shutdown
```

!The serial interfaces should remain shutdown until the Frame Relay
!switch is configured

```
interface loopback 0
ip address 209.165.200.225 255.255.255.224
router eigrp 1
no auto-summary
network 10.0.0.0
network 209.165.200.0
```

!

Task 3: Configure Frame Relay

You will now set up a basic point-to-point Frame Relay connection between routers 1 and 2. You first need to configure FR Switch as a Frame Relay switch and create DLCIs.

What does DLCI stand for?

What is a DLCI used for?

What is a PVC and how is it used?

Step 1: Configure FR Switch as a Frame Relay switch and create a PVC between R1 and R2.

This command enables Frame Relay switching globally on the router, allowing it to forward frames based on the incoming DLCI rather than on an IP address basis:

```
FR-Switch(config)#frame-relay switching
```

Change the interface encapsulation type to Frame Relay. Like HDLC or PPP, Frame Relay is a data link layer protocol that specifies the framing of Layer 2 traffic.

```
FR-Switch(config)#interface serial 0/0/0
```

```
FR-Switch(config)#clock rate 64000
```

```
FR-Switch(config-if)#encapsulation frame-relay
```

Changing the interface type to DCE tells the router to send LMI keepalives and allows Frame Relay route statements to be applied. You cannot set up PVCs using the **frame-relay route** command between two Frame Relay DTE interfaces.

```
FR-Switch(config-if)#frame-relay intf-type dce
```

Note: Frame Relay interface types do not need to match the underlying physical interface type. A physical DTE serial interface can act as a Frame Relay DCE interface, and a physical DCE interface can act as a logical Frame Relay DTE interface.

Configure the router to forward incoming traffic on interface serial 0/0/0 with DLCI 102 to serial 0/0/1 with an output DLCI of 201.

```
FR-Switch(config-if)#frame-relay route 102 interface serial 0/0/1 201
```

```
FR-Switch(config-if)#no shutdown
```

This configuration creates two PVCs: one from R1 to R2 (DLCI 102), and one from R2 to R1 (DLCI 201). You can verify the configuration using the **show frame-relay pvc** command.

```

FR-Switch(config-if)#interface serial 0/0/1
FR-Switch(config)#clock rate 64000
FR-Switch(config-if)#encapsulation frame-relay
FR-Switch(config-if)#frame-relay intf-type dce
FR-Switch(config-if)#frame-relay route 201 interface serial 0/0/0 102
FR-Switch(config-if)#no shutdown

```

```
FR-Switch#show frame-relay pvc
```

PVC Statistics for interface Serial0/0/0 (Frame Relay DCE)

	Active	Inactive	Deleted	Static
Local	0	0	0	0
Switched	0	1	0	0
Unused	0	0	0	0

DLCI = 102, DLCI USAGE = SWITCHED, PVC STATUS = INACTIVE, INTERFACE = Serial0/0/0

```

input pkts 0          output pkts 0          in bytes 0
out bytes 0          dropped pkts 0        in pkts dropped 0
out pkts dropped 0    out bytes dropped 0
in FECN pkts 0        in BECN pkts 0        out FECN pkts 0
out BECN pkts 0        in DE pkts 0          out DE pkts 0
out bcast pkts 0      out bcast bytes 0
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
switched pkts 0
Detailed packet drop counters:
no out intf 0          out intf down 0        no out PVC 0
in PVC down 0          out PVC down 0        pkt too big 0
shaping Q full 0       pkt above DE 0        policing drop 0
pvc create time 00:03:33, last time pvc status changed 00:00:19

```

PVC Statistics for interface Serial0/0/1 (Frame Relay DCE)

	Active	Inactive	Deleted	Static
Local	0	0	0	0
Switched	0	1	0	0
Unused	0	0	0	0

DLCI = 201, DLCI USAGE = SWITCHED, **PVC STATUS = INACTIVE**, INTERFACE = Serial0/0/1

```

input pkts 0          output pkts 0          in bytes 0
out bytes 0          dropped pkts 0        in pkts dropped 0
out pkts dropped 0    out bytes dropped 0
in FECN pkts 0        in BECN pkts 0        out FECN pkts 0
out BECN pkts 0        in DE pkts 0          out DE pkts 0
out bcast pkts 0      out bcast bytes 0
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
switched pkts 0
Detailed packet drop counters:
no out intf 0          out intf down 0        no out PVC 0

```

```

in PVC down 0          out PVC down 0          pkt too big 0
shaping Q full 0       pkt above DE 0         policing drop 0
pvc create time 00:02:02, last time pvc status changed 00:00:18

```

Notice the 1 in the Inactive column. The PVC you have created does not have any endpoints configured. The Frame Relay switch knows this and has marked the PVC as Inactive.

Issue the **show frame-relay route** command. This command shows any existing Frame Relay routes, their interfaces, DLCIs, and status. This is the Layer 2 route that Frame Relay traffic takes through the network. Do not confuse this with Layer 3 IP routing.

```
FR-Switch#show frame-relay route
```

Input Intf	Input DlcI	Output Intf	Output DlcI	Status
Serial0/0/0	102	Serial0/0/1	201	inactive
Serial0/0/1	201	Serial0/0/0	102	inactive

Step 2: Configure R1 for Frame Relay.

Inverse ARP allows distant ends of a Frame Relay link to dynamically discover each other and provides a dynamic method of mapping IP addresses to DLCIs. Although Inverse ARP is useful, it is not always reliable. The best practice is to statically map IP addresses to DLCIs and to disable inverse-arp.

```

R1(config)#interface serial 0/0/1
R1(config-if)#encapsulation frame-relay
R1(config-if)#no frame-relay inverse-arp

```

Why would you want to map an IP address to a DLCI?

The command **frame-relay map** statically maps an IP address to a DLCI. In addition to mapping IP to a DLCI, Cisco IOS software allows several other Layer 3 protocol addresses to be mapped. The **broadcast** keyword in the following command sends any multicast or broadcast traffic destined for this link over the DLCI. Most routing protocols require the **broadcast** keyword to properly function over Frame Relay. You can use the **broadcast** keyword on multiple DLCIs on the same interface. The traffic is replicated to all PVCs.

```
R1(config-if)#frame-relay map ip 10.1.1.2 102 broadcast
```

Is the DLCI mapped to the local IP address or the IP address at the other end of the PVC?

```
R1(config-if)#no shutdown
```

Why is the **no shutdown** command used after the **no frame-relay inverse-arp** command?

Step 3: Configure R2 for Frame Relay.

```
R2(config)#interface serial 0/0/1
R2(config-if)#encapsulation frame-relay
R2(config-if)#no frame-relay inverse-arp
R2(config-if)#frame-relay map ip 10.1.1.1 201 broadcast
R2(config-if)#no shutdown
```

At this point, you receive messages indicating that the interfaces have come up and that EIGRP neighbor adjacency has been established.

```
R1#*Sep  9 17:05:08.771: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
10.1.1.2 (Serial0/0/1) is up: new adjacency
```

```
R2#*Sep  9 17:05:47.691: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
10.1.1.1 (Serial0/0/1) is up: new adjacency
```

The **show ip route** command shows complete routing tables.

R1:

```
R1#show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
        level-2
        ia - IS-IS inter area, * - candidate default, U - per-user
        static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.10.0/24 is directly connected, FastEthernet0/0
D    209.165.200.0/24 [90/20640000] via 10.1.1.2, 00:00:07, Serial0/0/1
    10.0.0.0/30 is subnetted, 1 subnets
C      10.1.1.0 is directly connected, Serial0/0/1
```

R2:

```
R2#show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
```

```

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-
2
ia - IS-IS inter area, * - candidate default, U - per-user static
route
o - ODR, P - periodic downloaded static route

```

Gateway of last resort is not set

```

D   192.168.10.0/24 [90/20514560] via 10.1.1.1, 00:26:03, Serial0/0/1
    209.165.200.0/27 is subnetted, 1 subnets
C   209.165.200.224 is directly connected, Loopback0
    10.0.0.0/30 is subnetted, 1 subnets
C   10.1.1.0 is directly connected, Serial0/0/1

```

Task 4: Verify the Configuration

You should now be able to ping from R1 to R2. It may take several seconds after bringing up the interfaces for the PVC to become active. You can also see EIGRP routes for each router.

Step 1: Ping R1 and R2.

Ensure that you can ping router R2 from router R1.

R1#**ping 10.1.1.2**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms

R2#**ping 10.1.1.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms

Step 2: Get PVC information.

The **show frame-relay pvc** command displays information on all PVCs configured on the router. The output also includes the associated DLCI.

R1:

R1#**show frame-relay pvc**

PVC Statistics for interface Serial0/0/1 (Frame Relay DTE)

	Active	Inactive	Deleted	Static
Local	1	0	0	0
Switched	0	0	0	0
Unused	0	0	0	0

DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/1

```

input pkts 5          output pkts 5          in bytes 520
out bytes 520         dropped pkts 0         in pkts dropped 0
out pkts dropped 0    out bytes dropped 0
in FECN pkts 0       in BECN pkts 0       out FECN pkts 0
out BECN pkts 0      in DE pkts 0        out DE pkts 0
out bcast pkts 0     out bcast bytes 0
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 10:26:41, last time pvc status changed 00:01:04

```

R2:

R2#**show frame-relay pvc**

PVC Statistics for interface Serial0/0/1 (Frame Relay DTE)

	Active	Inactive	Deleted	Static
Local	1	0	0	0
Switched	0	0	0	0
Unused	0	0	0	0

DLCI = 201, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/1

```

input pkts 5          output pkts 5          in bytes 520
out bytes 520         dropped pkts 0         in pkts dropped 0
out pkts dropped 0    out bytes dropped 0
in FECN pkts 0       in BECN pkts 0       out FECN pkts 0
out BECN pkts 0      in DE pkts 0        out DE pkts 0
out bcast pkts 0     out bcast bytes 0
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 10:25:31, last time pvc status changed 00:00:00

```

FR Switch:

FR-Switch#**show frame-relay pvc**

PVC Statistics for interface Serial0/0/0 (Frame Relay DCE)

	Active	Inactive	Deleted	Static
Local	0	0	0	0
Switched	1	0	0	0
Unused	0	0	0	0

DLCI = 102, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0

```

input pkts 0          output pkts 0          in bytes 0
out bytes 0          dropped pkts 0         in pkts dropped 0
out pkts dropped 0    out bytes dropped 0
in FECN pkts 0       in BECN pkts 0       out FECN pkts 0
out BECN pkts 0      in DE pkts 0        out DE pkts 0
out bcast pkts 0     out bcast bytes 0
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec

```



```

switched pkts 0
Detailed packet drop counters:
no out intf 0          out intf down 0          no out PVC 0
in PVC down 0          out PVC down 0          pkt too big 0
shaping Q full 0       pkt above DE 0          policing drop 0
pvc create time 10:28:31, last time pvc status changed 00:03:57

```

PVC Statistics for interface Serial0/0/1 (Frame Relay DCE)

	Active	Inactive	Deleted	Static
Local	0	0	0	0
Switched	1	0	0	0
Unused	0	0	0	0

DLCI = 201, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/1

```

input pkts 0          output pkts 0          in bytes 0
out bytes 0           dropped pkts 0        in pkts dropped 0
out pkts dropped 0    out bytes dropped 0
in FECN pkts 0        in BECN pkts 0        out FECN pkts 0
out BECN pkts 0        in DE pkts 0          out DE pkts 0
out bcast pkts 0      out bcast bytes 0
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
switched pkts 0
Detailed packet drop counters:
no out intf 0          out intf down 0          no out PVC 0
in PVC down 0          out PVC down 0          pkt too big 0
shaping Q full 0       pkt above DE 0          policing drop 0
pvc create time 10:27:00, last time pvc status changed 00:04:03

```

Step 3: Verify Frame Relay mappings.

The **show frame-relay map** command displays information on the static and dynamic mappings of Layer 3 addresses to DLCIs. Because Inverse ARP has been turned off, there are only static maps.

R1:

R1#**show frame-relay map**

```

Serial0/0/1 (up): ip 10.1.1.2 dlci 102(0x66,0x1860), static,
                  CISCO, status defined, active

```

R2:

R2#**show frame-relay map**

```

Serial0/0/1 (up): ip 10.1.1.1 dlci 201(0xC9,0x3090), static,
                  CISCO, status defined, active

```

FR Switch:

FR Switch acts as a Layer 2 device, so there is no need to map Layer 3 addresses to Layer 2 DLCIs.

Step 4: Debug the Frame Relay LMI.

What purpose does the LMI serve in a Frame Relay network?

What are the three different types of LMI?

What DLCI does the LMI operate on?

Issue the **debug frame-relay lmi** command. The output gives detailed information on all LMI data. Keepalives are sent every 10 seconds, so you may have to wait until you see any output.

The debug output shows two LMI packets: the first outgoing, the second incoming.

```
R1#debug frame-relay lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
R1#
*Aug 24 06:19:15.920: Serial0/0/1(out): StEnq, myseq 196, yourseen
195, DTE up
*Aug 24 06:19:15.920: datagramstart = 0xE73F24F4, datagramsize = 13
*Aug 24 06:19:15.920: FR encap = 0xFCF10309
*Aug 24 06:19:15.920: 00 75 01 01 00 03 02 C4 C3
*Aug 24 06:19:15.920:
*Aug 24 06:19:15.924: Serial0/0/1(in): Status, myseq 196, pak size 21
*Aug 24 06:19:15.924: RT IE 1, length 1, type 0
*Aug 24 06:19:15.924: KA IE 3, length 2, yourseq 196, myseq 196
*Aug 24 06:19:15.924: PVC IE 0x7 , length 0x6 , dlci 102, status 0x2
, bw 0
R1#undebug all
Port Statistics for unclassified packets is not turned on.

All possible debugging has been turned off
```

Notice that the output shows an outgoing LMI packet with a sequence number of 196. The last LMI message received from the FR Switch had sequence number 195.

```
*Aug 24 06:19:15.920: Serial0/0/1(out): StEnq, myseq 196, yourseen
195, DTE up
```

This line indicates an incoming LMI message from the FR Switch to R1 with sequence number 196.

```
*Aug 24 06:19:15.924: Serial0/0/1(in): Status, myseq 196, pak size 21
FR Switch sent this as sequence number 196 (myseq), and the last LMI message received by the
FR-Switch from R1 had sequence number 196 (yourseq).
*Aug 24 06:19:15.924: KA IE 3, length 2, yourseq 196, myseq 196
DLCI 102 is the only DLCI on this link, and it is currently active.
*Aug 24 06:19:15.924: PVC IE 0x7 , length 0x6 , dlci 102, status 0x2
, bw 0
```

Task 4: Troubleshooting Frame Relay.

A variety of tools are available for troubleshooting Frame Relay connectivity issues. To learn about troubleshooting, you will break the Frame Relay connection established earlier and then re-establish it.

Step 1: Remove the frame map from R1.

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface serial0/0/1
R1(config-if)#encapsulation frame-relay
R1(config-if)#no frame-relay map ip 10.1.1.2 102 broadcast
```

Now that you have removed the frame map statement from R1, try to ping router R1 from router R2. You will get no response.

```
R2#ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Additionally, you should get console messages reporting the EIGRP adjacency going up and down.

```
R1(config-if)#*Sep 9 17:28:36.579: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1:
Neighbor 10.1.1.2 (Serial0/0/1) is down: Interface Goodbye received
R1(config-if)#*Sep 9 17:29:32.583: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1:
Neighbor 10.1.1.2 (Serial0/0/1) is up: new adjacency
R1(config-if)#*Sep 9 17:32:37.095: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1:
Neighbor 10.1.1.2 (Serial0/0/1) is down: retry limit exceeded
R2#*Sep 9 17:29:15.359: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
10.1.1.1 (Serial0/0/1) is down: holding time expired
```

Issue the **debug ip icmp** command on R1:

```
R1#debug ip icmp
ICMP packet debugging is on
```

Now ping the serial interface of R1 again. The following debug message appears on R1:

```
R2#ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
```

.....

Success rate is 0 percent (0/5)

R1#*Sep 9 17:42:13.415: ICMP: echo reply sent, src 10.1.1.1, dst 10.1.1.2

R1#*Sep 9 17:42:15.411: ICMP: echo reply sent, src 10.1.1.1, dst 10.1.1.2

R1#*Sep 9 17:42:17.411: ICMP: echo reply sent, src 10.1.1.1, dst 10.1.1.2

R1#*Sep 9 17:42:19.411: ICMP: echo reply sent, src 10.1.1.1, dst 10.1.1.2

R1#*Sep 9 17:42:21.411: ICMP: echo reply sent, src 10.1.1.1, dst 10.1.1.2

As is shown by this debug message, the ICMP packet from R2 is reaching R1.

Why does the ping fail?

Issuing the **show frame-relay map** command returns a blank line.

R1#**show frame-relay map**

R1#

Turn off all debugging with the **undebug all** command, and re-apply the **frame-relay map ip** command but without using the **broadcast** keyword.

R1#undebug all

Port Statistics for unclassified packets is not turned on.

All possible debugging has been turned off

R1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#**interface serial0/0/1**

R1(config-if)#**encapsulation frame-relay**

R1(config-if)#**frame-relay map ip 10.1.1.2 102**

R2#ping 10.1.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 40/41/44 ms

Notice that while pings are successful, the EIGRP adjacency continues to “flap” (go up and down).

R1(config-if)#*Sep 9 17:47:58.375: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.2 (Serial0/0/1) is **up: new adjacency**

R1(config-if)#*Sep 9 17:51:02.887: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.2 (Serial0/0/1) is **down: retry limit exceeded**

R1(config-if)#*Sep 9 17:51:33.175: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.2 (Serial0/0/1) is **up: new adjacency**

```
R1(config-if)#Sep  9 17:54:37.687: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1:
Neighbor 10.1.1.2 (Serial0/0/1) is down: retry limit exceeded
```

Why does the EIGRP adjacency continue to flap?

Replace the Frame Relay map statement and include the **broadcast** keyword this time. Verify that the full routing table is restored and that you have full end-to-end connectivity.

```
R1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
R1(config)#interface serial0/0/1
```

```
R1(config-if)#encapsulation frame-relay
```

```
R1(config-if)#frame-relay map ip 10.1.1.2 102 broadcast
```

```
R1#show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
static route o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.10.0/24 is directly connected, FastEthernet0/0
    209.165.200.0/27 is subnetted, 1 subnets
D    209.165.200.224 [90/20640000] via 10.1.1.2, 00:00:05, Serial0/0/1
    10.0.0.0/30 is subnetted, 1 subnets
C    10.1.1.0 is directly connected, Serial0/0/1
```

Step 2: Change the Frame Relay encapsulation type.

Cisco IOS software supports two types of Frame Relay encapsulation: the default Cisco encapsulation and the standards-based IETF encapsulation. Change the Frame Relay encapsulation on serial0/0/1 on R2 to IETF.

```
R2(config-if)#encapsulation frame-relay ietf
```

Notice that the interface does not go down. You might be surprised by this. Cisco routers can correctly interpret Frame Relay frames that use either the default Cisco Frame Relay encapsulation or the IETF standard Frame Relay encapsulation. If your network is composed entirely of Cisco routers, then it does not make any difference whether you use the default Cisco Frame Relay encapsulation or the IETF standard. Cisco routers understand both types of incoming frames. However, if you have routers from different vendors using Frame Relay, then the IETF standard must be used. The command **encapsulation frame-relay ietf** forces the Cisco router to encapsulate its outgoing frames using the IETF standard. This standard can be correctly understood by the router of another vendor.

```
R2#show interface serial 0/0/1
```

```
Serial0/0/1 is up, line protocol is up
```

```
Hardware is GT96K Serial
Internet address is 10.1.1.2/30
MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation FRAME-RELAY IETF, loopback not set
```

<output omitted>

```
FR-Switch#show int s0/0/0
Serial0/0/0 is up, line protocol is up
Hardware is GT96K Serial
MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation FRAME-RELAY, loopback not set
```

Note the difference in output between the two **show interface** commands. Also notice that the EIGRP adjacency is still up. Although FR Switch and R2 are using different encapsulation types, they are still passing traffic.

Change the encapsulation type back to the default:

```
R2(config-if)#encapsulation frame-relay
```

Step 3: Change the LMI type.

On R2, change the LMI type to ANSI.

```
R2#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
R2(config)#interface serial 0/0/1
R2(config-if)#encapsulation frame-relay
R2(config-if)#frame-relay lmi-type ansi
R2(config-if)#^Z
R2#copy run start
```

Destination filename [startup-config]?

Building configuration...

[OK]

```
*Sep  9 18:41:08.351: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
```

```
*Sep  9 18:41:08.351: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
10.1.1.1 (Serial0/0/1) is down: interface down
```

```
R2#show interface serial 0/0/1
```

```
Serial0/0/1 is up, line protocol is down
```

```
R2#show frame-relay lmi
```

```
LMI Statistics for interface Serial0/0/1 (Frame Relay DTE) LMI TYPE =
ANSI
```

Invalid Unnumbered info 0	Invalid Prot Disc 0
Invalid dummy Call Ref 0	Invalid Msg Type 0
Invalid Status Message 0	Invalid Lock Shift 0
Invalid Information ID 0	Invalid Report IE Len 0
Invalid Report Request 0	Invalid Keep IE Len 0
Num Status Enq. Sent 1391	Num Status msgs Rcvd 1382
Num Update Status Rcvd 0	Num Status Timeouts 10

Last Full Status Req 00:00:27

Last Full Status Rcvd 00:00:27

If you continue issuing the **show frame-relay lmi** command, you will notice the highlighted times incrementing. When 60 seconds have passed, the interface changes its state to Up Down, because R2 and FR Switch are no longer exchanging keepalives or any other link-state information.

Issue the **debug frame-relay lmi** command. Notice that LMI packets are no longer showing up in pairs. While all outgoing LMI messages are logged, no incoming messages are shown. This is because R2 is expecting ANSI LMI, and FR Switch is sending Cisco LMI.

R2#**debug frame-relay lmi**

```
*Aug 25 04:34:25.774: Serial0/0/1(out): StEnq, myseq 20, yourseen 0,
DTE down
*Aug 25 04:34:25.774: datagramstart = 0xE73F2634, datagramsize = 14
*Aug 25 04:34:25.774: FR encap = 0x00010308
*Aug 25 04:34:25.774: 00 75 95 01 01 00 03 02 14 00
*Aug 25 04:34:25.774:
```

Leave debugging on and restore the LMI type to Cisco on R2.

R2(config-if)#**frame-relay lmi-type cisco**

```
*Aug 25 04:42:45.774: Serial0/0/1(out): StEnq, myseq 2, yourseen 1, DTE
down
*Aug 25 04:42:45.774: datagramstart = 0xE7000D54, datagramsize = 13
*Aug 25 04:42:45.774: FR encap = 0xFCF10309
*Aug 25 04:42:45.774: 00 75 01 01 01 03 02 02 01
*Aug 25 04:42:45.774:
*Aug 25 04:42:45.778: Serial0/0/1(in): Status, myseq 2, pak size 21
*Aug 25 04:42:45.778: RT IE 1, length 1, type 0
*Aug 25 04:42:45.778: KA IE 3, length 2, yourseq 2 , myseq 2
*Aug 25 04:42:45.778: PVC IE 0x7 , length 0x6 , dlci 201, status 0x2 ,
bw 0
*Aug 25 04:42:55.774: Serial0/0/1(out): StEnq, myseq 3, yourseen 2, DTE
up
*Aug 25 04:42:55.774: datagramstart = 0xE7001614, datagramsize = 13
*Aug 25 04:42:55.774: FR encap = 0xFCF10309
*Aug 25 04:42:55.774: 00 75 01 01 01 03 02 03 02
*Aug 25 04:42:55.774:
*Aug 25 04:42:55.778: Serial0/0/1(in): Status, myseq 3, pak size 21
*Aug 25 04:42:55.778: RT IE 1, length 1, type 0
*Aug 25 04:42:55.778: KA IE 3, length 2, yourseq 1 , myseq 3
*Aug 25 04:42:55.778: PVC IE 0x7 , length 0x6 , dlci 201, status 0x2 ,
bw 0
*Aug 25 04:42:56.774: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
```

As you can see, the LMI sequence number has been reset to 1, and R2 began to understand the LMI messages coming in from FR Switch. After FR Switch and R2 had successfully exchanged LMI messages, the interface changed state to Up.

Task 5: Configure a Frame Relay Sub-interface

Frame Relay supports two types of sub-interfaces: point-to-point and point-to-multipoint. Point-to-multipoint sub-interfaces support non-broadcast multi-access topologies. For example, a hub and

spoke topology would use a point-to-multipoint sub-interface. In this lab, you will create a point-to-point sub-interface.

Step 1: On FR Switch, create a new PVC between R1 and R2.

```
FR-Switch(config)#interface serial 0/0/0
FR-Switch(config-if)#frame-relay route 112 interface serial 0/0/1 212
FR-Switch(config-if)#interface serial 0/0/1
FR-Switch(config-if)#frame-relay route 212 interface serial 0/0/0 112
```

Step 2: Create and configure a point-to-point sub-interface on R1.

Create subinterface 112 as a point-to-point interface. Frame Relay encapsulation must be specified on the physical interface before subinterfaces can be created.

```
R1(config)#interface serial 0/0/1.112 point-to-point
R1(config-subif)#ip address 10.1.1.5 255.255.255.252
R1(config-subif)#frame-relay interface-dlci 112
```

Step 3: Create and configure a point-to-point sub-interface on R2.

```
R2(config)#interface serial 0/0/1.212 point-to-point
R2(config-subif)#ip address 10.1.1.6 255.255.255.252
R2(config-subif)#frame-relay interface-dlci 212
```

Step 4: Verify connectivity.

You should be able to ping across the new PVC.

```
R1#ping 10.1.1.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
```

```
R2#ping 10.1.1.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
```

You can also verify the configuration using the **show frame-relay pvc** and **show frame-relay map** commands in Task 4.

R1:

```
R1#show frame-relay pvc
```

PVC Statistics for interface Serial0/0/1 (Frame Relay DTE)

	Active	Inactive	Deleted	Static
Local	2	0	0	0
Switched	0	0	0	0
Unused	0	0	0	0

```
DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial0/0/1
```



```

input pkts 319          output pkts 279          in bytes 20665
out bytes 16665         dropped pkts 0          in pkts dropped 0
out pkts dropped 0      out bytes dropped 0
in FECN pkts 0         in BECN pkts 0         out FECN pkts 0
out BECN pkts 0        in DE pkts 0          out DE pkts 0
out bcast pkts 193     out bcast bytes 12352
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 04:43:35, last time pvc status changed 01:16:05

```

DLCI = 112, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial0/0/1.112

```

input pkts 15          output pkts 211         in bytes 2600
out bytes 17624         dropped pkts 0          in pkts dropped 0
out pkts dropped 0      out bytes dropped 0
in FECN pkts 0         in BECN pkts 0         out FECN pkts 0
out BECN pkts 0        in DE pkts 0          out DE pkts 0
out bcast pkts 200     out bcast bytes 16520
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 00:19:16, last time pvc status changed 00:18:56

```

R2:

R2#**show frame-relay pvc**

PVC Statistics for interface Serial0/0/1 (Frame Relay DTE)

	Active	Inactive	Deleted	Static
Local	2	0	0	0
Switched	0	0	0	0
Unused	0	0	0	0

DLCI = 201, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial0/0/1

```

input pkts 331          output pkts 374          in bytes 19928
out bytes 24098         dropped pkts 0          in pkts dropped 0
out pkts dropped 0      out bytes dropped 0
in FECN pkts 0         in BECN pkts 0         out FECN pkts 0
out BECN pkts 0        in DE pkts 0          out DE pkts 0
out bcast pkts 331     out bcast bytes 21184
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 05:22:55, last time pvc status changed 01:16:36

```

DLCI = 212, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial0/0/1.212

```

input pkts 217          output pkts 16          in bytes 18008
out bytes 2912         dropped pkts 0          in pkts dropped 0
out pkts dropped 0      out bytes dropped 0
in FECN pkts 0         in BECN pkts 0         out FECN pkts 0
out BECN pkts 0        in DE pkts 0          out DE pkts 0
out bcast pkts 6       out bcast bytes 1872

```

```

5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 00:19:37, last time pvc status changed 00:18:57

```

FR Switch:

```
FR-Switch#show frame-relay pvc
```

PVC Statistics for interface Serial0/0/0 (Frame Relay DCE)

	Active	Inactive	Deleted	Static
Local	0	0	0	0
Switched	2	0	0	0
Unused	0	0	0	0

DLCI = 102, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0

```

input pkts 335          output pkts 376          in bytes 20184
out bytes 24226         dropped pkts 2          in pkts dropped 2
out pkts dropped 0      out bytes dropped 0
in FECN pkts 0         in BECN pkts 0         out FECN pkts 0
out BECN pkts 0        in DE pkts 0           out DE pkts 0
out bcast pkts 0       out bcast bytes 0
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
switched pkts 333
Detailed packet drop counters:
no out intf 0          out intf down 0        no out PVC 0
in PVC down 0          out PVC down 2         pkt too big 0
shaping Q full 0       pkt above DE 0         policing drop 0
pvc create time 05:23:43, last time pvc status changed 01:18:32

```

DLCI = 112, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0

```

input pkts 242          output pkts 18          in bytes 20104
out bytes 3536         dropped pkts 0          in pkts dropped 0
out pkts dropped 0      out bytes dropped 0
in FECN pkts 0         in BECN pkts 0         out FECN pkts 0
out BECN pkts 0        in DE pkts 0           out DE pkts 0
out bcast pkts 0       out bcast bytes 0
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
switched pkts 242
Detailed packet drop counters:
no out intf 0          out intf down 0        no out PVC 0
in PVC down 0          out PVC down 0         pkt too big 0
shaping Q full 0       pkt above DE 0         policing drop 0
pvc create time 00:21:41, last time pvc status changed 00:21:22

```

PVC Statistics for interface Serial0/0/1 (Frame Relay DCE)

	Active	Inactive	Deleted	Static
Local	0	0	0	0
Switched	2	0	0	0

Unused	0	0	0	0
--------	---	---	---	---

DLCI = 201, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/1

```

input pkts 376          output pkts 333          in bytes 24226
out bytes 20056         dropped pkts 0          in pkts dropped 0
out pkts dropped 0      out bytes dropped 0
in FECN pkts 0         in BECN pkts 0        out FECN pkts 0
out BECN pkts 0        in DE pkts 0         out DE pkts 0
out bcast pkts 0       out bcast bytes 0
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
switched pkts 376
Detailed packet drop counters:
no out intf 0          out intf down 0          no out PVC 0
in PVC down 0          out PVC down 0          pkt too big 0
shaping Q full 0      pkt above DE 0         policing drop 0
pvc create time 05:23:14, last time pvc status changed 01:39:39

```

DLCI = 212, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/1

```

input pkts 18           output pkts 243        in bytes 3536
out bytes 20168         dropped pkts 0          in pkts dropped 0
out pkts dropped 0      out bytes dropped 0
in FECN pkts 0         in BECN pkts 0        out FECN pkts 0
out BECN pkts 0        in DE pkts 0         out DE pkts 0
out bcast pkts 0       out bcast bytes 0
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
switched pkts 18
Detailed packet drop counters:
no out intf 0          out intf down 0          no out PVC 0
in PVC down 0          out PVC down 0          pkt too big 0
shaping Q full 0      pkt above DE 0         policing drop 0
pvc create time 00:21:36, last time pvc status changed 00:21:20

```

R1:

R1#**show frame-relay map**

```

Serial0/0/1 (up): ip 10.1.1.2 dlci 102(0x66,0x1860), static,
                  broadcast,
                  CISCO, status defined, active
Serial0/0/1.112 (up): point-to-point dlci, dlci 112(0x70,0x1C00),
broadcast
                  status defined, active

```

R2:

R2#**show frame-relay map**

```

Serial0/0/1 (up): ip 10.1.1.1 dlci 201(0xC9,0x3090), static,
                  broadcast,
                  CISCO, status defined, active

```

```
Serial0/0/1.212 (up): point-to-point dlci, dlci 212(0xD4,0x3440),
broadcast
                status defined, active
```

FR Switch:

```
FR-Switch#show frame-relay route
```

Input Intf	Input Dlci	Output Intf	Output Dlci	Status
Serial0/0/0	102	Serial0/0/1	201	active
Serial0/0/0	112	Serial0/0/1	212	active
Serial0/0/1	201	Serial0/0/0	102	active
Serial0/0/1	212	Serial0/0/0	112	active

Now debug the Frame Relay LMI.

```
R1#debug frame-relay lmi
```

```
*Aug 25 05:58:50.902: Serial0/0/1(out): StEnq, myseq 136, yourseen 135,
DTE up
*Aug 25 05:58:50.902: datagramstart = 0xE7000354, datagramsize = 13
*Aug 25 05:58:50.902: FR encap = 0xFCF10309
*Aug 25 05:58:50.902: 00 75 01 01 00 03 02 88 87
*Aug 25 05:58:50.902:
*Aug 25 05:58:50.906: Serial0/0/1(in): Status, myseq 136, pak size 29
*Aug 25 05:58:50.906: RT IE 1, length 1, type 0
*Aug 25 05:58:50.906: KA IE 3, length 2, yourseq 136, myseq 136
*Aug 25 05:58:50.906: PVC IE 0x7 , length 0x6 , dlci 102, status 0x2 ,
bw 0
*Aug 25 05:58:50.906: PVC IE 0x7 , length 0x6 , dlci 112, status 0x2 ,
bw 0
```

Note that two DLCIs are listed in the LMI message from FR Switch to R1.

```
R2#debug frame-relay lmi
```

```
*Aug 25 06:08:35.774: Serial0/0/1(out):StEnq, myseq 7,yourseen 4,DTE up
*Aug 25 06:08:35.774: datagramstart = 0xE73F28B4, datagramsize = 13
*Aug 25 06:08:35.774: FR encap = 0xFCF10309
*Aug 25 06:08:35.774: 00 75 01 01 00 03 02 07 04
*Aug 25 06:08:35.774:
*Aug 25 06:08:35.778: Serial0/0/1(in): Status, myseq 7, pak size 29
*Aug 25 06:08:35.778: RT IE 1, length 1, type 0
*Aug 25 06:08:35.778: KA IE 3, length 2, yourseq 5 , myseq 7
*Aug 25 06:08:35.778: PVC IE 0x7,length 0x6, dlci 201, status 0x2, bw 0
*Aug 25 06:08:35.778: PVC IE 0x7,length 0x6, dlci 212, status 0x2, bw 0
```

Final Configurations

```
R1#show run
<output omitted>
!
hostname R1

enable secret class
no ip domain lookup
!
```

```
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 no shutdown
!
interface Serial0/0/1
 ip address 10.1.1.1 255.255.255.252
 encapsulation frame-relay
 frame-relay map ip 10.1.1.2 102 broadcast
 no frame-relay inverse-arp
 no shutdown
!
interface Serial0/0/1.112 point-to-point
 ip address 10.1.1.5 255.255.255.252
 frame-relay interface-dlci 112
!
router eigrp 1
 network 10.0.0.0
 network 192.168.10.0
 no auto-summary
!
!
banner motd ^CUnauthorized access prohibited, violators will be
prosecuted to the full extent of the law.^C
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 login
 password cisco
!
end
```

```
R2#show run
<output omitted>
!
hostname R2
!
!
enable secret class
!
!
no ip domain lookup
!
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
!
interface Serial0/0/1
 ip address 10.1.1.2 255.255.255.252
 encapsulation frame-relay
 clockrate 64000
```

```
frame-relay map ip 10.1.1.1 201 broadcast
no frame-relay inverse-arp
frame-relay lmi-type cisco
no shutdown
!
interface Serial0/0/1.212 point-to-point
ip address 10.1.1.6 255.255.255.252
frame-relay interface-dlci 212
!
router eigrp 1
network 10.0.0.0
network 209.165.200.224 0.0.0.31
no auto-summary
!
!
line con 0
password cisco
logging synchronous
login
line aux 0
line vty 0 4
password cisco
login
!
end

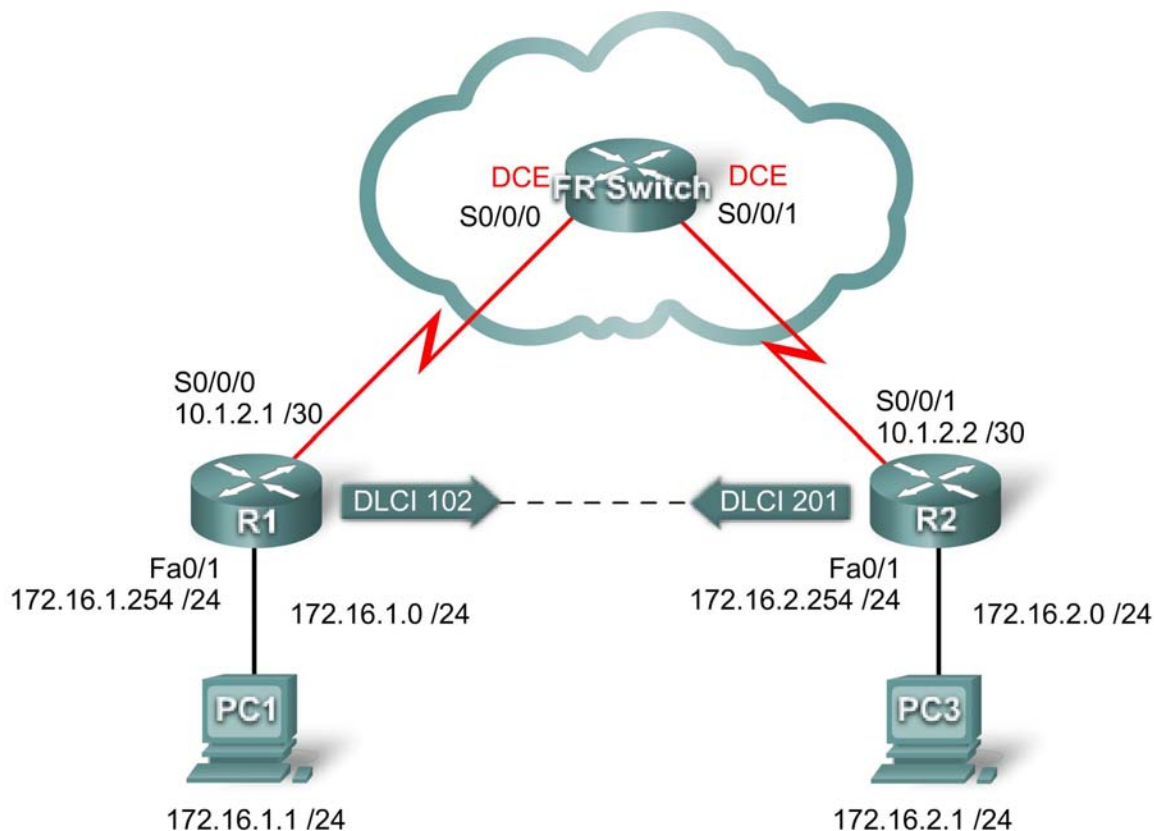
FR-Switch#show run
<output omitted>
!
hostname FR-Switch
!
enable secret class
!
no ip domain lookup
frame-relay switching
!
!
!
!
interface Serial0/0/0
no ip address
encapsulation frame-relay

clockrate 64000
frame-relay intf-type dce
frame-relay route 102 interface Serial0/0/1 201
frame-relay route 112 interface Serial0/0/1 212
no shutdown
!
interface Serial0/0/1
no ip address
encapsulation frame-relay
frame-relay intf-type dce
frame-relay route 201 interface Serial0/0/0 102
frame-relay route 212 interface Serial0/0/0 112
no shutdown
```

```
!  
!  
line con 0  
  password cisco  
  login  
line aux 0  
line vty 0 4  
  password cisco  
  login  
!  
end
```

Lab 3.5.2: Challenge Frame Relay Configuration

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1	172.16.1.254	255.255.255.0	N/A
	S0/0/0	10.1.2.1	255.255.255.252	N/A
R2	Fa0/1	172.16.2.254	255.255.255.0	N/A
	S0/0/1	10.1.2.2	255.255.255.252	N/A
PC1	NIC	172.16.1.1	255.255.255.0	172.16.1.254
PC3	NIC	172.16.2.1	255.255.255.0	172.16.2.254

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram

- Erase the startup configuration and reload a router to the default state
- Perform basic configuration tasks on a router
- Configure and activate interfaces
- Configure EIGRP routing on all routers
- Configure Frame Relay encapsulation on all serial interfaces
- Configure a Frame Relay PVC
- Intentionally break and restore a Frame Relay PVC
- Configure Frame Relay subinterfaces
- Intentionally break and restore the PVC

Scenario

In this lab, you will configure Frame Relay using the network shown in the topology diagram. If you need assistance, refer to the Basic Frame Relay lab. However, try to do as much on your own as possible.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configuration

Configure the R1, R2, and R3 routers according to the following guidelines:

- Configure the router hostname.
- Disable DNS lookup.
- Configure an EXEC mode password.
- Configure a message-of-the-day banner.
- Configure a password for console connections.
- Configure synchronous logging.
- Configure a password for vty connections.

Task 3: Configure IP Addresses

Step 1: Configure IP addresses on all links according to the addressing table.

Step 2: Verify IP addressing and interfaces.

Step 3: Activate Ethernet interfaces of R1 and R2. Do not activate the serial interfaces.

Step 3: Configure the Ethernet interfaces of PC1 and PC3.

Step 4: Test connectivity between the PCs and their local routers.

Task 4: Configure EIGRP on Routers R1 and R2

Step 1: Enable EIGRP on R1 and R2 for all subnets.

Task 5: Configure Frame Relay PVC Between R1 and R2

Step 1: Configure interfaces on FR-Switch to create the PVC between R1 and R2.

Use the DLCIs in the topology diagram.

Step 2: Configure physical interfaces on R1 and R2 for Frame Relay encapsulation.

Do not automatically discover IP addresses on the far end of links. Activate the link after full configuration.

Step 3: Configure Frame Relay maps on R1 and R2 with proper DLCIs. Enable broadcast traffic on the DLCIs.

Step 4: Verify end-to-end connectivity using PC1 and PC2.

Task 6: Intentionally Break the PVC and Then Restore It

Step 1: By a means of your choosing, break the PVC between R1 and R2.

Step 2: Restore full connectivity to your network.

Step 3: Verify full connectivity to your network.

Task 7: Configure Frame Relay Subinterfaces

Step 1: Remove the IP address and frame map configuration from the physical interfaces on R1 and R2.

Step 2: Configure Frame Relay point-to-point subinterfaces on R1 and R2 with the same IP addresses and DLCI used earlier on the physical interfaces.

Step 3: Verify full end-to-end connectivity.

Task 8: Intentionally Break the PVC and Then Restore It

Step 1: Break the PVC using a different method than you used in Task 6.

Step 2: Restore the PVC.

Step 3: Verify full end-to-end connectivity.

Task 9: Document the Router Configurations

On each router, issue the **show run** command and capture the configurations.

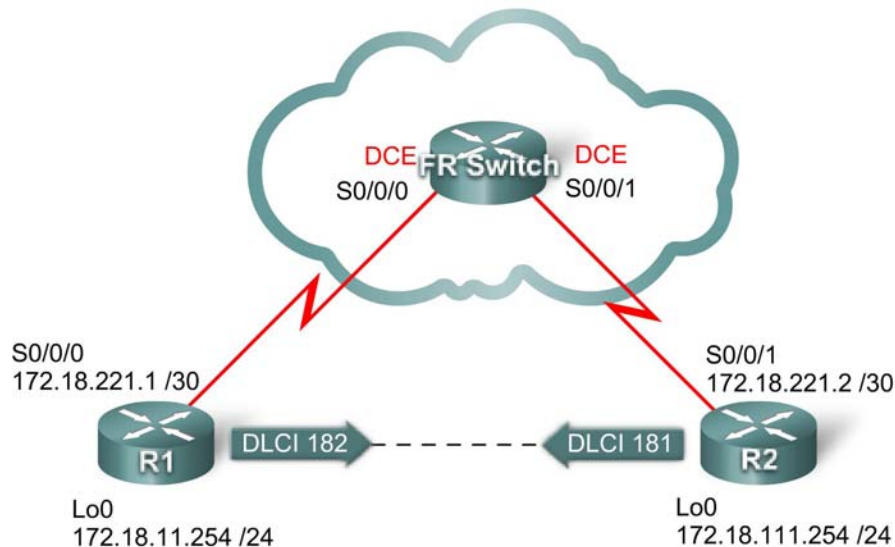
Task 10: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts

that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 3.5.3: Troubleshooting Frame Relay

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Lo0	172.18.11.254	255.255.255.0	N/A
	S0/0/0	172.18.221.1	255.255.255.252	N/A
R2	Lo0	172.18.111.254	255.255.255.0	N/A
	S0/0/1	172.18.221.2	255.255.255.252	N/A

Learning Objectives

Practice Frame Relay troubleshooting skills.

Scenario

In this lab, you will practice troubleshooting a misconfigured Frame Relay environment. Load or have your instructor load the configurations below into your routers. Locate and repair all errors in the configurations and establish end-to-end connectivity. Your final configuration should match the topology diagram and addressing table. All passwords are set to **cisco** except the enable secret password which is set to **class**.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

Step 2: Clear any existing configurations on the routers.

Step 3: Import the configurations.

Router 1

```
!  
hostname R1  
!  
enable secret class  
!  
no ip domain lookup  
!  
!  
!  
interface Loopback0  
  ip address 172.18.11.254 255.255.255.0  
!  
interface FastEthernet0/0  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
!  
interface FastEthernet0/1  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
!  
interface Serial0/0/1  
  no ip address  
  shutdown  
  no fair-queue  
  clockrate 125000  
!  
interface Serial0/0/0  
  ip address 172.18.221.1 255.255.255.252  
  encapsulation frame-relay  
  frame-relay map ip 172.18.221.2 678 broadcast  
  no frame-relay inverse-arp  
  no shutdown  
!  
router eigrp 1  
  network 172.18.221.0  
  network 172.18.11.0  
  no auto-summary  
!  
!  
!  
line con 0
```

```
password cisco
logging synchronous
line aux 0
line vty 0 4
password cisco
login
!
end
```

Router 2

```
!
hostname R2
!
enable secret class
!
no ip domain lookup
!
interface Loopback0
ip address 172.18.111.254 255.255.255.0
!
interface FastEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
no fair-queue
!
interface Serial0/0/1
ip address 172.18.221.2 255.255.255.252
encapsulation frame-relay
clockrate 125000
frame-relay map ip 172.18.221.1 181
no frame-relay inverse-arp
frame-relay lmi-type ansi
!
router eigrp 1
network 172.18.221.0
network 172.18.111.0
no auto-summary
!
!
!
line con 0
password cisco
logging synchronous
line aux 0
```

```
line vty 0 4
  login
!
end

FR-Switch:
!
hostname FR-Switch
!
!
enable secret class
!
!
!
no ip domain lookup
frame-relay switching
!
!
!
!
interface FastEthernet0/0
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface Serial0/0/0
  no ip address
  encapsulation frame-relay
  no fair-queue
  clockrate 125000
  frame-relay intf-type dce
  frame-relay route 182 interface Serial0/0/1 181
  no shutdown
!
interface Serial0/0/1
  no ip address
  clockrate 125000
  encapsulation frame-relay
  frame-relay intf-type dce
  no shutdown
!
!
!
!
line con 0
  password cisco
  logging synchronous
line aux 0
line vty 0 4
```

```
password cisco
login
!
end
```

Task 2: Troubleshoot and Repair the Frame Relay Connection Between R1 and R2.

Task 3: Document the Router Configurations

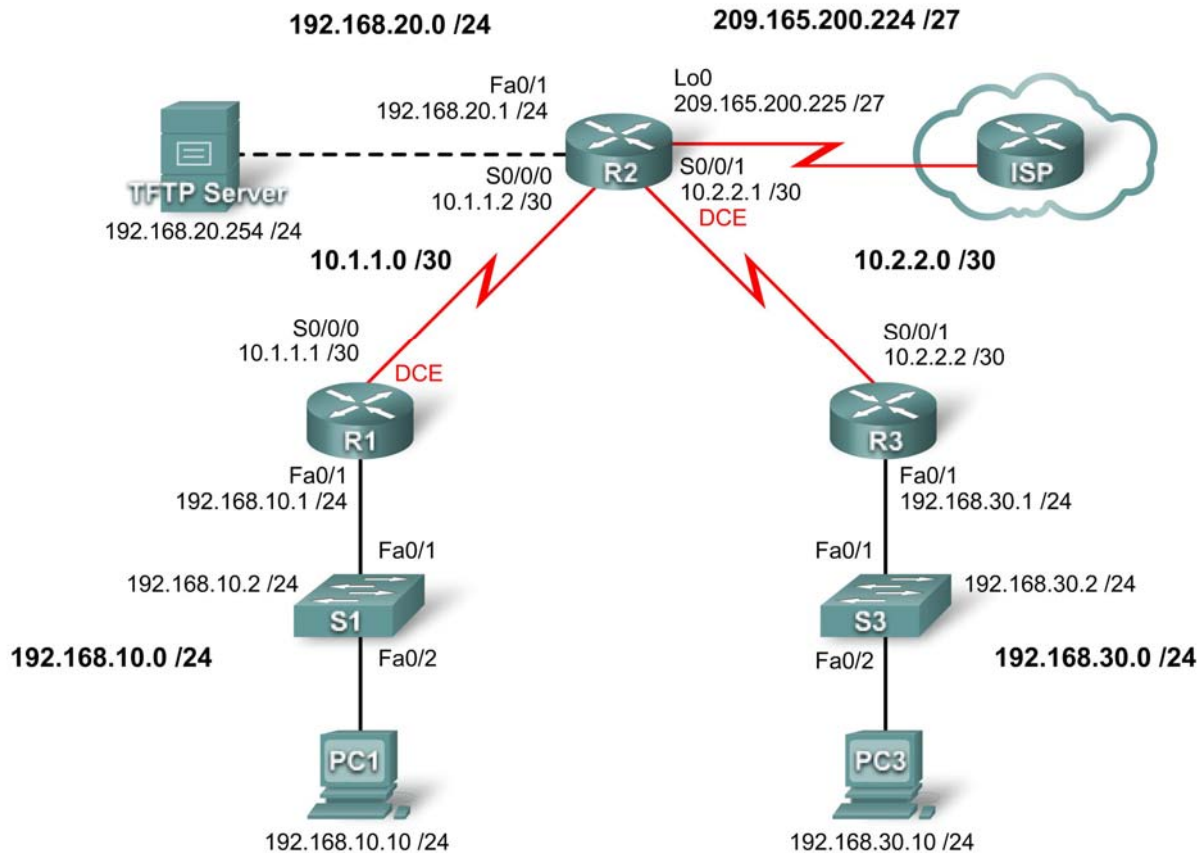
On each router, issue the **show run** command and capture the configurations.

Task 4: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks, such as the school LAN or to the Internet, reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 4.6.1: Basic Security Configuration

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1	192.168.10.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	Fa0/1	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
R3	Fa0/1	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
S1	VLAN10	192.168.10.2	255.255.255.0	N/A

S3	VLAN20	192.168.30.2	255.255.255.0	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
TFTP Server	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Perform basic configuration tasks on a router
- Configure basic router security
- Disable unused Cisco services and interfaces
- Protect enterprise networks from basic external and internal attacks
- Understand and manage Cisco IOS configuration files and Cisco file system
- Set up and use Cisco SDM (Security Device Manager) and SDM Express to configure basic router security
- Configure VLANs on the switches

Scenario

In this lab, you will learn how to configure basic network security using the network shown in the topology diagram. You will learn how to configure router security three different ways: using the CLI, the auto-secure feature, and Cisco SDM. You will also learn how to manage Cisco IOS software.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

Note: This lab was developed and tested using 1841 routers. If you use 1700, 2500, or 2600 series routers, the router outputs and interface descriptions might be different.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configurations

Step 1: Configure routers.

Configure the R1, R2, and R3 routers according to the following guidelines:

- Configure the router hostname according to the topology diagram.
- Disable DNS lookup.
- Configure a message of the day banner.
- Configure IP addresses on R1, R2, and R3.
- Enable RIP version 2 on all routers for all networks.

- Create a loopback interface on R2 to simulate the connection to the Internet.
- Configure a TFTP server on R2. If you need to download TFTP server software, one option is: <http://tftpd32.jounin.net/>

Step 2: Configure Ethernet interfaces.

Configure the Ethernet interfaces of PC1, PC3, and TFTP Server with the IP addresses and default gateways from the Addressing Table at the beginning of the lab.

Step 3: Test the PC configuration by pinging the default gateway from each of the PCs and the TFTP server.

Task 3: Secure the Router from Unauthorized Access

Step 1: Configure secure passwords and AAA authentication.

Use a local database on R1 to configure secure passwords. Use **ciscoccna** for all passwords in this lab.

```
R1(config)#enable secret ciscoccna
```

How does configuring an enable secret password help protect a router from being compromised by an attack?

The **username** command creates a username and password that is stored locally on the router. The default privilege level of the user is 0 (the least amount of access). You can change the level of access for a user by adding the keyword **privilege 0-15** before the **password** keyword.

```
R1(config)#username ccna password ciscoccna
```

The **aaa** command enables AAA (authentication, authorization, and accounting) globally on the router. This is used when connecting to the router.

```
R1(config)#aaa new-model
```

You can create an authentication list that is accessed when someone attempts to log in to the device after applying it to vty and console lines. The **local** keyword indicates that the user database is stored locally on the router.

```
R1(config)#aaa authentication login LOCAL_AUTH local
```

The following commands tell the router that users attempting to connect to the router should be authenticated using the list you just created.

```
R1(config)#line console 0
R1(config-lin)#login authentication LOCAL_AUTH
R1(config-lin)#line vty 0 4
R1(config-lin)#login authentication LOCAL_AUTH
```

What do you notice that is insecure about the following section of the running configuration:

```
R1#show run
<output omitted>
!
enable secret 5 $1$.DB7$DunHvguQH0EvLqzQCqzfr1
!
aaa new-model
!
aaa authentication login LOCAL_AUTH local
!
username ccna password 0 ciscoccna
!
<output omitted>
!
banner motd ^CUnauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law^C
!
line con 0
  logging synchronous
  login authentication LOCAL_AUTH
line aux 0
line vty 0 4
  login authentication LOCAL_AUTH
!
```

To apply simple encryption to the passwords, enter the following command in global config mode:

```
R1(config)#service password-encryption
```

Verify this with the **show run** command.

```
R1#show run
service password-encryption
!
enable secret 5 $1$.DB7$DunHvguQH0EvLqzQCqzfr1
!
aaa new-model
!
aaa authentication login LOCAL_AUTH local
!
username ccna password 7 0822455D0A1606141C0A
<output omitted>
!
banner motd ^CCUnauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law^C
!
line con 0
  logging synchronous
  login authentication LOCAL_AUTH
line aux 0
```

```
line vty 0 4
 login authentication LOCAL_AUTH
!
```

Step 2: Secure the console and VTY lines.

You can cause the router to log out a line that has been idle for a specified time. If a network engineer was logged into a networking device and was suddenly called away, this command automatically logs the user out after the specified time. The following commands cause the line to log out after 5 minutes.

```
R1(config)#line console 0
R1(config-lin)#exec-timeout 5 0
R1(config-lin)#line vty 0 4
R1(config-lin)#exec-timeout 5 0
```

The following command hampers brute force login attempts. The router blocks login attempts for 5 minutes if someone fails five attempts within 2 minutes. This is set especially low for the purpose of this lab. An additional measure is to log each time this happens.

```
R1(config)#login block-for 300 attempt 2 within 120
R1(config)#security authentication failure rate 5 log
```

To verify this, attempt to connect to R1 from R2 via Telnet with an **incorrect username and password.**

On R2:

```
R2#telnet 10.1.1.1
Trying 10.1.1.1 ... Open
Unauthorized access strictly prohibited, violators will be prosecuted to the
full extent of the law

User Access Verification

Username: cisco
Password:

% Authentication failed

User Access Verification

Username: cisco
Password:

% Authentication failed

[Connection to 10.1.1.1 closed by foreign host]
R2#telnet 10.1.1.1
Trying 10.1.1.1 ...
% Connection refused by remote host
```

On R1:

```
*Sep 10 12:40:11.211: %SEC_LOGIN-5-QUIET_MODE_OFF: Quiet Mode is OFF, because
block period timed out at 12:40:11 UTC Mon Sep 10 2007
```

Task 4: Secure Access to the Network

Step 1: Prevent RIP routing update propagation.

Who can receive RIP updates on a network segment where RIP is enabled? Is this the most desirable setup?

The **passive-interface** command prevents routers from sending routing updates to all interfaces except those interfaces configured to participate in routing updates. This command is issued as part of the RIP configuration.

The first command puts all interfaces into passive mode (the interface only receives RIP updates). The second command returns specific interfaces from passive to active mode (both sending and receiving RIP updates).

R1

```
R1(config)#router rip
R1(config-router)#passive-interface default
R1(config-router)#no passive-interface s0/0/0
```

R2

```
R2(config)#router rip
R2(config-router)#passive-interface default
R2(config-router)#no passive-interface s0/0/0
R2(config-router)#no passive-interface s0/0/1
```

R3

```
R3(config)#router rip
R3(config-router)#passive-interface default
R3(config-router)#no passive-interface s0/0/1
```

Step 2: Prevent unauthorized reception of RIP updates.

Preventing unnecessary RIP updates to the whole network is the first step to securing RIP. The next is to have RIP updates password protected. To do this, you must first configure a key to use.

```
R1(config)#key chain RIP_KEY
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string cisco
```

This has to be added to each router that is going to receive RIP updates.

```
R2(config)#key chain RIP_KEY
R2(config-keychain)#key 1
R2(config-keychain-key)#key-string cisco
```

```
R3(config)#key chain RIP_KEY
R3(config-keychain)#key 1
R3(config-keychain-key)#key-string cisco
```

To use the key, each interface participating in RIP updates needs to be configured. These will be the same interfaces that were enabled using the **no passive-interface** command earlier.

R1

```
R1(config)#int s0/0/0
R1(config-if)#ip rip authentication mode md5
R1(config-if)#ip rip authentication key-chain RIP_KEY
```

At this point, R1 is no longer receiving RIP updates from R2, because R2 is not yet configured to use a key for routing updates. You can view this on R1 using the **show ip route** command and confirming that no routes from R2 appear in the routing table.

Clear out IP routes with **clear ip route *** or wait for routes to timeout.

R1#show ip route

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, *- candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

Gateway of last resort is not set

```
      10.0.0.0/8 is variably subnetted, 1 subnets, 1 masks
C       10.1.1.0/24 is directly connected, Serial0/0/0
C      192.168.10.0 is directly connected, Serial0/0/0
```

Configure R2 and R3 to use routing authentication. Remember that each active interface must be configured.

R2

```
R2(config)#int s0/0/0
R2(config-if)#ip rip authentication mode md5
R2(config-if)#ip rip authentication key-chain RIP_KEY
R2(config)#int s0/0/1
R2(config-if)#ip rip authentication mode md5
R2(config-if)#ip rip authentication key-chain RIP_KEY
```

R3

```
R3(config)#int s0/0/1
R3(config-if)#ip rip authentication mode md5
R3(config-if)#ip rip authentication key-chain RIP_KEY
```

Step 3: Verify that RIP routing still works.

After all three routers have been configured to use routing authentication, the routing tables should repopulate with all RIP routes. R1 should now have all the routes via RIP. Confirm this with the **show ip route** command.

R1#show ip route

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, *-candidate default, U-per-user static route
       o - ODR, P - periodic downloaded static route
```

Gateway of last resort is not set

```
R    192.168.30.0/24 [120/2] via 10.1.1.2, 00:00:16, Serial0/0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/1
R    192.168.20.0/24 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 1 masks
R    10.2.2.0/24 [120/1] via 10.1.0.2, 00:00:16, Serial0/0/0
C    10.1.1.0/24 is directly connected, Serial0/0/0
```

Task 5: Logging Activity with SNMP (Simple Network Management Protocol)

Step 1: Configure SNMP logging to the syslog server.

SNMP logging can be useful in monitoring network activity. The captured information can be sent to a syslog server on the network, where it can be analyzed and archived. You should be careful when configuring logging (syslog) on the router. When choosing the designated log host, remember that the log host should be connected to a trusted or protected network or an isolated and dedicated router interface.

In this lab, you will configure PC1 as the syslog server for R1. Use the `logging` command to select the IP address of the device to which SNMP messages are sent. In this example, the IP address of PC1 is used.

```
R1(config)#logging 192.168.10.10
```

Note: PC1 should have syslog software installed and running if you wish to view syslog messages.

In the next step, you will define the level of severity for messages to be sent to the syslog server.

Step 2: Configure the SNMP severity level.

The level of SNMP messages can be adjusted to allow the administrator to determine what kinds of messages are sent to the syslog device. Routers support different levels of logging. The eight levels range from 0 (emergencies), indicating that the system is unstable, to 7 (debugging), which sends messages that include router information. To configure the severity levels, you use the keyword associated with the level, as shown in the table.

Severity Level	Keyword	Description
0	emergencies	System unusable
1	alerts	Immediate action required
2	critical	Critical conditions
3	errors	Error conditions
4	warnings	Warning conditions
5	notifications	Normal but significant condition
6	informational	Informational messages
7	debugging	Debugging messages

The `logging trap` command sets the severity level. The severity level includes the level specified and anything below it (severity-wise). Set R1 to level 4 to capture messages with severity level 4, 5, 6, and 7.


```
R1(config)#logging trap warnings
```

What is the danger of setting the level of severity too high or too low?

Note: If you installed syslog software on PC1, generate and look at syslog software for messages.

Task 6: Disabling Unused Cisco Network Services

Step 1: Disable unused interfaces.

Why should you disable unused interfaces on network devices?

In the topology diagram, you can see that R1 should only be using interface S0/0/0 and Fa0/1. All other interfaces on R1 should be administratively shut down using the **shutdown** interface configuration command.

```
R1(config)#interface fastethernet0/0
R1(config-if)#shutdown
R1(config-if)# interface s0/0/1
R1(config-if)#shutdown
```

```
*Sep 10 13:40:24.887: %LINK-5-CHANGED: Interface FastEthernet0/0, changed
state to administratively down
*Sep 10 13:40:25.887: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to down
```

To verify that R1 has all inactive interfaces shut down, use the **show ip interface brief** command. Interfaces manually shut down are listed as administratively down.

```
R1#sh ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	administratively down	down
FastEthernet0/1	192.168.10.1	YES	manual	up	up
Serial0/0/0	10.1.0.1	YES	manual	up	up
Serial0/0/1	unassigned	YES	unset	administratively down	down

Step 2: Disable unused global services.

Many services are not needed in most modern networks. Leaving unused services enabled leaves ports open that can be used to compromise a network. Disable each of these services on R1.

```
R1(config)#no service pad
R1(config)#no service finger
R1(config)#no service udp-small-server
R1(config)#no service tcp-small-server
```

```
R1(config)#no ip bootp server
R1(config)#no ip http server
R1(config)#no ip finger
R1(config)#no ip source-route
R1(config)#no ip gratuitous-arps
R1(config)#no cdp run
```

Step 3: Disable unused interface services.

These commands are entered at the interface level and should be applied to every interface on R1.

```
R1(config-if)#no ip redirects
R1(config-if)#no ip proxy-arp
R1(config-if)#no ip unreachable
R1(config-if)#no ip directed-broadcast
R1(config-if)#no ip mask-reply
R1(config-if)#no mop enabled
```

What kind of attack does disabling IP redirects, IP unreachables, and IP directed broadcasts mitigate?

Step 4: Use AutoSecure to secure a Cisco router.

By using a single command in CLI mode, the AutoSecure feature allows you to disable common IP services that can be exploited for network attacks and enable IP services and features that can aid in the defense of a network when under attack. AutoSecure simplifies the security configuration of a router and hardens the router configuration.

Using the AutoSecure feature, you can apply the same security features that you just applied (except for securing RIP) to a router much faster. Because you have already secured R1, use the **auto secure** command on R3.

```
R3#auto secure
```

```
--- AutoSecure Configuration ---
```

```
*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***
```

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.

At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

```
Is this router connected to internet? [no]: yes
Enter the number of interfaces facing the internet [1]: 1
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	down	down
FastEthernet0/1	192.168.30.1	YES	manual	up	up
Serial0/0/0	unassigned	YES	manual	down	down
Serial0/0/1	10.2.2.2	YES	manual	up	up

Enter the interface name that is facing the internet: **Serial0/0/1**
Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp
Enable secret is either not configured or
Is the same as enable password
Enter the new enable password: **ciscoccna**
Confirm the enable password: **ciscoccna**
Enter the new enable password: **ccnacisco**
Confirm the enable password: **ccnacisco**

Configuration of local user database
Enter the username: **ccna**
Enter the password: **ciscoccna**
Confirm the password: **ciscoccna**
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected: **300**

Maximum Login failures with the device: **5**

Maximum time period for crossing the failed login attempts: **120**

Configure SSH server? **Yes**
Enter domain-name: **cisco.com**

Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:

no ip redirects
no ip proxy-arp
no ip unreachable
no ip directed-broadcast
no ip mask-reply

Disabling mop on Ethernet interfaces

Securing Forwarding plane services...

Enabling CEF (This might impact the memory requirements for your platform)
Enabling unicast rpf on all interfaces connected to internet

Configure CBAC firewall feature: **no**

Tcp intercept feature is used prevent tcp syn attack

On the servers in the network. Create autosec_tcp_intercept_list

To form the list of servers to which the tcp traffic is to be observed

Enable TCP intercept feature: **yes**

This is the configuration generated:

```
no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
security passwords min-length 6
security authentication failure rate 10 log
enable password 7 070C285F4D061A061913
username ccna password 7 045802150C2E4F4D0718
aaa new-model
aaa authentication login local_auth local
line con 0
  login authentication local_auth
  exec-timeout 5 0
  transport output telnet
line aux 0
  login authentication local_auth
  exec-timeout 10 0
  transport output telnet
line vty 0 4
  login authentication local_auth
  transport input telnet
line tty 1
  login authentication local_auth
  exec-timeout 15 0
line tty 192
  login authentication local_auth
  exec-timeout 15 0
login block-for 300 attempts 5 within 120
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

```
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface FastEthernet0/0
  no ip redirects
  no ip proxy-arp
  no ip unreachable
  no ip directed-broadcast
  no ip mask-reply
  no mop enabled
interface FastEthernet0/1
  no ip redirects
  no ip proxy-arp
  no ip unreachable
  no ip directed-broadcast
  no ip mask-reply
  no mop enabled
interface Serial0/0/0
  no ip redirects
  no ip proxy-arp
  no ip unreachable
  no ip directed-broadcast
  no ip mask-reply
interface Serial0/0/1
  no ip redirects
  no ip proxy-arp
  no ip unreachable
  no ip directed-broadcast
  no ip mask-reply
interface Serial0/1/0
  no ip redirects
  no ip proxy-arp
  no ip unreachable
  no ip directed-broadcast
  no ip mask-reply
interface Serial0/1/1
  no ip redirects
  no ip proxy-arp
  no ip unreachable
  no ip directed-broadcast
  no ip mask-reply
ip cef
access-list 100 permit udp any any eq bootpc
interface Serial0/0/1
  ip verify unicast source reachable-via rx allow-default 100
ip tcp intercept list autosec_tcp_intercept_list
ip tcp intercept drop-mode random
ip tcp intercept watch-timeout 15
ip tcp intercept connection-timeout 3600
ip tcp intercept max-incomplete low 450
ip tcp intercept max-incomplete high 550
!
end
```

Apply this configuration to running-config? [yes]:**yes**

The name for the keys will be: R3.cisco.com

```
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R3#
000045: *Nov 16 15:39:10.991 UTC: %AUTOSEC-1-MODIFIED: AutoSecure
configuration has been Modified on this device
```

As you can see, the AutoSecure feature is much faster than line by line configuration. However, there are advantages to doing it manually, as you will see in the troubleshooting lab. When you use AutoSecure, you may disable a service you need. Always use caution and think about the services that you require before using AutoSecure.

Task 7: Managing Cisco IOS and Configuration Files

Step 1: Show Cisco IOS files.

Cisco IOS is the software that routers use to operate. Your router may have enough memory to store multiple Cisco IOS images. It is important to know which files are stored on your router.

Issue the **show flash** command to view the contents of the flash memory of your router.

Caution: Be very careful when issuing commands that involve the flash memory. Mistyping a command could result in the deletion of the Cisco IOS image.

```
R2#show flash
-#- --length-- -----date/time----- path
1      13937472 May 05 2007 21:25:14 +00:00 c1841-ipbase-mz.124-1c.bin
2          1821 May 05 2007 21:40:28 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:41:02 +00:00 sdm.tar
4      833024 May 05 2007 21:41:24 +00:00 es.tar
5      1052160 May 05 2007 21:41:48 +00:00 common.tar

8679424 bytes available (23252992 bytes used)
```

Just by looking at this list, we can determine the following:

- The image is for an 1841 router (c**1841**-ipbase-mz.124-1c.bin).
- The router is using IP base image (c**1841-ipbase**-mz.124-1c.bin).
- The Cisco IOS is version 12.4(1c) (c1841-ipbase-mz.**124-1c**.bin).
- SDM is installed on this device (**sdmconfig**-18xx.cfg, **sdm**.tar).

You can use the **dir all** command to show all files on the router.

```
R2#dir all
Directory of archive:/

No files in directory

No space information available
Directory of system:/

 3  dr-x          0          <no date>  memory
 1  -rw-        979          <no date>  running-config
 2  dr-x          0          <no date>  vfiles
```

No space information available
Directory of nvram:/

```

189  -rw-          979          <no date>  startup-config
190  ----          5          <no date>  private-config
191  -rw-          979          <no date>  underlying-config
   1  -rw-          0          <no date>  ifIndex-table

```

196600 bytes total (194540 bytes free)
Directory of flash:/

```

 1 -rw- 13937472  May 05 2007 20:08:50 +00:00 c1841-ipbase-mz.124-1c.bin
 2 -rw-    1821  May 05 2007 20:25:00 +00:00 sdmconfig-18xx.cfg
 3 -rw- 4734464  May 05 2007 20:25:38 +00:00 sdm.tar
 4 -rw-  833024  May 05 2007 20:26:02 +00:00 es.tar
 5 -rw- 1052160  May 05 2007 20:26:30 +00:00 common.tar
 6 -rw-   1038   May 05 2007 20:26:56 +00:00 home.shtml
 7 -rw-  102400  May 05 2007 20:27:20 +00:00 home.tar
 8 -rw-  491213  May 05 2007 20:27:50 +00:00 128MB.sdf
 9 -rw-  398305  May 05 2007 20:29:08 +00:00 sslclient-win-1.1.0.154.pkg
10 -rw- 1684577  May 05 2007 20:28:32 +00:00 securedesktop-ios-3.1.1.27-
k9.pkg

```

31932416 bytes total (8679424 bytes free)

Step 2: Transfer files with TFTP.

TFTP is used when archiving and updating the Cisco IOS software of a device. In this lab, however, we do not use actual Cisco IOS files because any mistakes made in entering the commands could lead to erasing the Cisco IOS image of the device. At the end of this section, there is an example of what a Cisco IOS TFTP transfer looks like.

Why is it important to have an updated version of Cisco IOS software?

When transferring files via TFTP, it is important to ensure that the TFTP server and the router can communicate. One way to test this is to ping between these devices.

To begin transfer of the Cisco IOS software, create a file on the TFTP server called **test** in the TFTP root folder. This file can be a blank text file, because this step only serves to illustrate the steps involved. Each TFTP program differs in where files are stored. Consult your TFTP server help file to determine the root folder.

From R1, retrieve the file and save it to the flash memory.

R2#**copy tftp flash**

Address or name of remote host []? **192.168.20.254** (IP address of the TFTP server)

Source filename []? **test** (name of the file you created and saved to TFTP server)

Destination filename [test]? **test-server** (An arbitrary name for the file when saved to the router)

Accessing tftp://192.168.20.254/test...

Loading test from 192.168.20.254 (via FastEthernet0/1): !

```
[OK - 1192 bytes]
```

```
1192 bytes copied in 0.424 secs (2811 bytes/sec)
```

Verify the file's existence in the flash with the **show flash** command.

```
R2#show flash
```

```
-#- --length-- -----date/time----- path
1      13937472 May 05 2007 21:13:20 +00:00 c1841-ipbase-mz.124-1c.bin
2          1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4      833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6          1038 May 05 2007 21:31:36 +00:00 home.shtml
7      102400 May 05 2007 21:32:02 +00:00 home.tar
8      491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10     398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg
11     1192 Sep 12 2007 07:38:18 +00:00 test-server
```

```
8675328 bytes available (23257088 bytes used)
```

Routers can also act as TFTP servers. This can be useful if there is a device that needs an image and you have one that is already using that image. We will make R2 a TFTP server for R1. Remember that Cisco IOS images are specific to router platforms and memory requirements. Use caution when transferring a Cisco IOS image from one router to another.

The command syntax is: **tftp-server nvram: [filename1 [alias filename2]]**

The command below configures R2 as a TFTP server. R2 supplies its startup config file to devices requesting it via TFTP (we are using the startup config for the sake of simplicity and ease). The **alias** keyword allows devices to request the file using the alias **test** instead of the full filename.

```
R2(config)#tftp-server nvram:startup-config alias test
```

Now we can request the file from R2 using R1.

```
R1#copy tftp flash
```

```
Address or name of remote host []? 10.1.1.2
Source filename []? test
Destination filename []? test-router
Accessing tftp://10.1.1.2/test...
Loading test from 10.1.1.2 (via Serial0/0/0): !
[OK - 1192 bytes]
```

```
1192 bytes copied in 0.452 secs (2637 bytes/sec)
```

Again, verify that the file **test** has been successfully copied with the **show flash** command

```
R1#show flash
```

```
-#- --length-- -----date/time----- path
1      13937472 May 05 2007 21:13:20 +00:00 c1841-ipbase-mz.124-1c.bin
2          1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4      833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6          1038 May 05 2007 21:31:36 +00:00 home.shtml
7      102400 May 05 2007 21:32:02 +00:00 home.tar
```



```
8      491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10     398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg
11      1192 Sep 12 2007 07:38:18 +00:00 test-server
12     1192 Sep 12 2007 07:51:04 +00:00 test-router
```

8671232 bytes available (23261184 bytes used)

Because you do not want unused files occupying precious memory space, delete them now from the flash memory of R1. **Be very careful when doing this!** Accidentally erasing flash memory will mean that you have to re-install the entire IOS image for the router. If the router prompts you to **erase flash**, something is very wrong. You rarely want to erase the entire flash. The only legitimate time this will happen is when you are upgrading the IOS to a large IOS image. If you see the **erase flash** prompt as in the example, STOP IMMEDIATELY. Do NOT hit enter. IMMEDIATELY ask for assistance from your instructor.

```
Erase flash: ?[confirm] no
```

```
R1#delete flash:test-server
Delete filename [test-server]?
Delete flash:test? [confirm]
R1#delete flash:test-router
Delete filename [test-router]?
Delete flash:test-router? [confirm]
```

Verify that the files have been deleted by issuing the **show flash** command. **This is an example only. Do not complete this task.**

```
R1#show flash
#- --length-- ----date/time----- path
1      13937472 May 05 2007 21:13:20 +00:00 c1841-ipbase-mz.124-1c.bin
2          1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4      833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6          1038 May 05 2007 21:31:36 +00:00 home.shtml
7      102400 May 05 2007 21:32:02 +00:00 home.tar
8      491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10     398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg
```

8679424 bytes available (23252992 bytes used)

The following is an example of a TFTP transfer of a Cisco IOS image file.

Do NOT complete on your routers. Only read it.

```
R1#copy tftp flash
Address or name of remote host []? 10.1.1.2
Source filename []? c1841-ipbase-mz.124-1c.bin
Destination filename []? flash:c1841-ipbase-mz.124-1c.bin
Accessing tftp://10.1.1.2/c1841-ipbase-mz.124-1c.bin...
Loading c1841-ipbase-mz.124-1c.bin from 10.1.1.2 (via Serial0/0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 13937472 bytes]
```

13937472 bytes copied in 1113.948 secs (12512 bytes/sec)

Step 3: Recover a password using ROMmon.

If for some reason you can no longer access a device because you do not know, have lost, or have forgotten a password, you can still gain access by changing the configuration register. The configuration register tells the router which configuration to load on bootup. In the configuration register, you can instruct the router to boot from a blank configuration that is not password protected.

The first step in changing the configuration register is to view the current setting using the **show version** command. These steps are performed on R3.

R3#**show version**

```
Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.4(1c), RELEASE
SOFTWARE (fc1)
```

```
Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 1986-2005 by Cisco Systems, Inc.
```

```
Compiled Tue 25-Oct-05 17:10 by evmiller
```

```
ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
```

```
R3 uptime is 25 minutes
```

```
System returned to ROM by reload at 08:56:50 UTC Wed Sep 12 2007
```

```
System image file is "flash:c1841-ipbase-mz.124-1c.bin"
```

```
Cisco 1841 (revision 7.0) with 114688K/16384K bytes of memory.
```

```
Processor board ID FTX1118X0BN
```

```
2 FastEthernet interfaces
```

```
2 Low-speed serial(sync/async) interfaces
```

```
DRAM configuration is 64 bits wide with parity disabled.
```

```
191K bytes of NVRAM.
```

```
31360K bytes of ATA CompactFlash (Read/Write)
```

Configuration register is 0x2102

Next, reload the router and send a break during the boot up. The **Break** key is different on different computers. Frequently, it is in the upper right hand corner of the keyboard. A break causes the device to enter a mode called ROMmon. This mode does not require the device to have access to a Cisco IOS image file.

R3#**reload**

```
Proceed with reload? [confirm]
```

```
*Sep 12 08:27:28.670: %SYS-5-RELOAD: Reload requested by console. Reload
```

```
Reason: Reload command.
```

```
System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
```

```
Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 2006 by cisco Systems, Inc.
```

```
PLD version 0x10
```

```
GIO ASIC version 0x127
```

```
c1841 platform with 131072 Kbytes of main memory
```

```
Main memory is configured to 64 bit mode with parity disabled
```

```
Readonly ROMMON initialized
```

```
rommon 1 >
```

Change the configuration register to a value that loads the initial configuration of the router. This configuration does not have a password configured, but supports Cisco IOS commands. Change the value of the configuration register to 0x2142.

```
rommon 1 > confreg 0x2142
```

Now that this is changed we can boot the device with the **reset** command.

```
rommon 2 > reset
```

```
program load complete, entry point: 0x8000f000, size: 0xcb80
```

```
program load complete, entry point: 0x8000f000, size: 0xcb80
```

```
program load complete, entry point: 0x8000f000, size: 0xd4a9a0
```

```
Self decompressing the image :
```

```
#####
```

```
#####
```

```
# [OK]
```

```
<output omitted>
```

```
--- System Configuration Dialog ---
```

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

Press RETURN to get started!

Step 4: Restore the router.

Now we copy the startup configuration to the running configuration, restore the configuration, and then change the configuration register back to the default (0x2102).

To copy the startup configuration from NVRAM to running memory, type **copy startup-config running-config**. Be careful! Do *not* type **copy running-config startup-config** or you will erase your startup configuration.

```
Router#copy startup-config running-config
```

```
Destination filename [running-config]? {enter}
```

```
2261 bytes copied in 0.576 secs (3925 bytes/sec)
```

```
R3#show running-config
```

```
<output omitted>
```

```
enable secret 5 $1$31P/$cyPgoxc0R9y93Ps/N3/kg.
```

```
!
```

```
<output omitted>
```

```
!
```

```
key chain RIP_KEY
```

```
key 1
```

```
key-string 7 01100F175804
```

```
username ccna password 7 094F471A1A0A1411050D
```

```
!
```

```
interface FastEthernet0/1
```

```
ip address 192.168.30.1 255.255.255.0
```

```
no ip redirects
no ip unreachable
no ip proxy-arp
no ip directed-broadcast
shutdown
duplex auto
speed auto
!
interface Serial0/0/1
ip address 10.2.2.2 255.255.255.252
no ip redirects
no ip unreachable
no ip proxy-arp
no ip directed-broadcast
shutdown
ip rip authentication mode md5
ip rip authentication key-chain RIP_KEY
!
<output omitted>
!
line con 0
exec-timeout 5 0
logging synchronous
login authentication
transport output telnet
line aux 0
exec-timeout 15 0
logging synchronous
login authentication local_auth
transport output telnet
line vty 0 4
exec-timeout 15 0
logging synchronous
login authentication local_auth
transport input telnet
!
end
```

In this configuration, the **shutdown** command appears under all interfaces because all the interfaces are currently shut down. Most important, you can now see the passwords (enable password, enable secret, VTY, console passwords) in either an encrypted or unencrypted format. You can reuse unencrypted passwords. You must change encrypted passwords to a new password.

R3#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

```
R3(config)#enable secret ciscocna
```

```
R3(config)#username ccna password ciscocna
```

Issue the **no shutdown** command on every interface that you want to use.

```
R3(config)#interface FastEthernet0/1
```

```
R3(config-if)#no shutdown
```

```
R3(config)#interface Serial0/0/0
```

```
R3(config-if)#no shutdown
```

You can issue a **show ip interface brief** command to confirm that your interface configuration is correct. Every interface that you want to use should display up up.

R3#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	NVRAM	administratively down	down
FastEthernet0/1	192.168.30.1	YES	NVRAM	up	up
Serial0/0/0	10.2.2.2	YES	NVRAM	up	up
Serial0/0/1	unassigned	YES	NVRAM	administratively down	down

Type **config-register** *configuration register value*. The variable *configuration register value* is either the value you recorded in Step 3 or 0x2102. Save the running configuration.

R3(config)#config-register 0x2102

R3(config)#end

R3#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

What are the downsides to password recovery?

Task 8: Using SDM to Secure a Router

In this task, you will use Security Device Manager (SDM), the GUI interface, to secure router R2. SDM is faster than typing each command and gives you more control than the AutoSecure feature.

Verify whether SDM is installed on your router:

R2#show flash

```

-#- --length-- -----date/time----- path
1      13937472 Sep 12 2007 08:31:42 +00:00 c1841-ipbase-mz.124-1c.bin
2          1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4      833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6          1038 May 05 2007 21:31:36 +00:00 home.shtml
7      102400 May 05 2007 21:32:02 +00:00 home.tar
8       491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10      398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg
11         2261 Sep 25 2007 23:20:16 +00:00 Tr(RIP)
12       2506 Sep 26 2007 17:11:58 +00:00 save.txt

```

If SDM is NOT installed on your router, it must be installed to continue. Please consult your instructor for directions.

Step 1: Connect to R2 using TFTP Server.

Create a username and password on R2.

R2(config)#username ccna password ciscoccna

Enable the http secure server on R2 and connect to R2 using a web browser on TFTP Server.

```
R2(config)#ip http secure-server
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R2(config)#
*Nov 16 16:01:07.763: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Nov 16 16:01:08.731: %PKI-4-NOAUTOSAVE: Configuration was modified. Issue
"write memory" to save new certificate
R2(config)#end
R2#copy run start
```

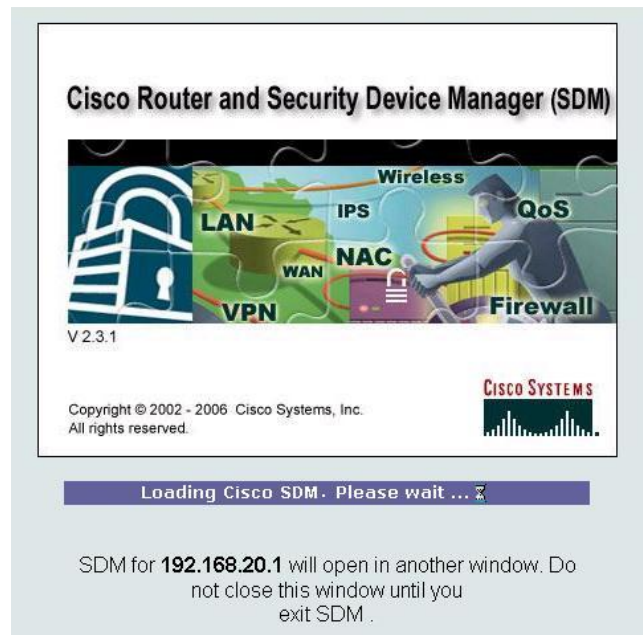
From TFTP Server, open a web browser and navigate to <https://192.168.20.1/>. Login with the previously configured username and password:

username: **ccna**

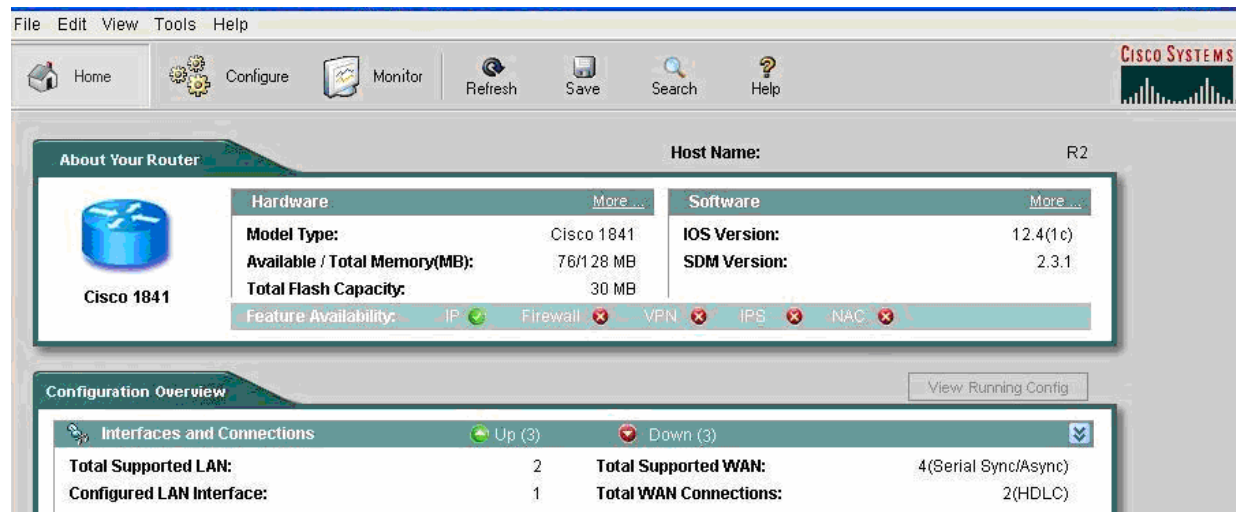
password: **ciscoccna**

Select **Cisco Router and Security Device Manager**

Open Internet Explorer and enter the IP address for R2 in the address bar. A new window opens. Make sure that you have all popup blockers turned off in your browser. Also make sure that JAVA is installed and updated.

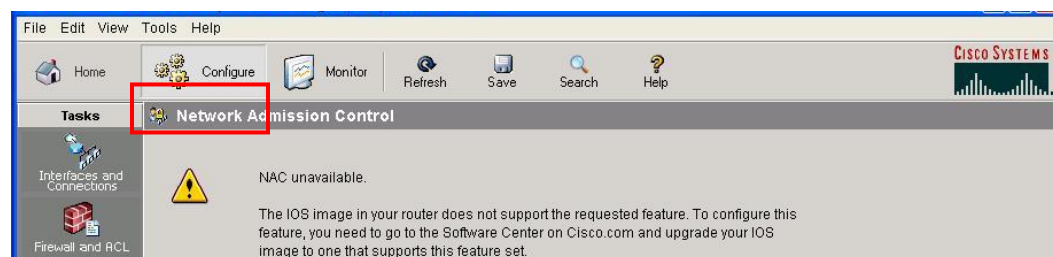


After it is done loading, a new window opens for SDM.

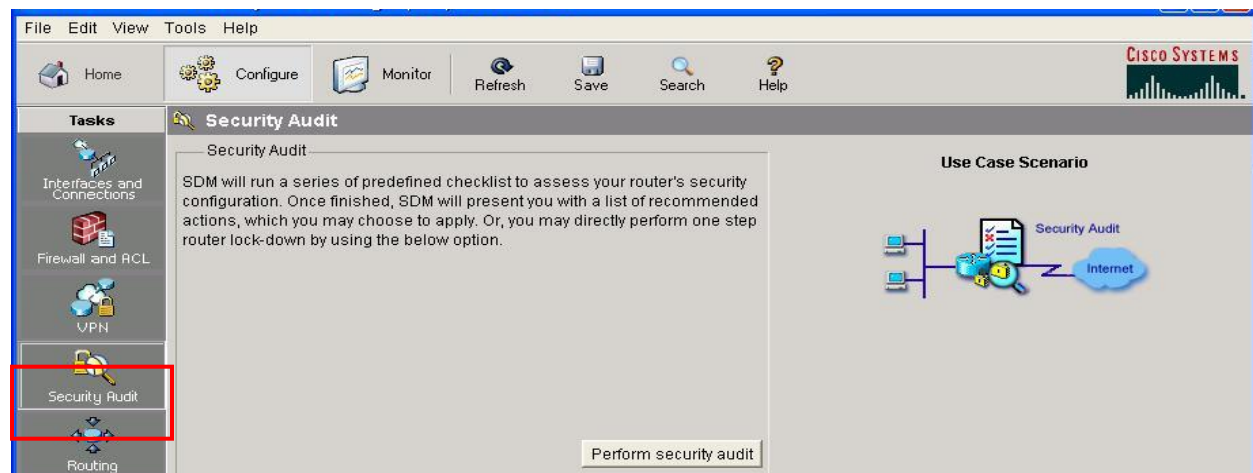


Step 2: Navigate to the Security Audit feature.

Click the **Configure** button in the top left side of the window.

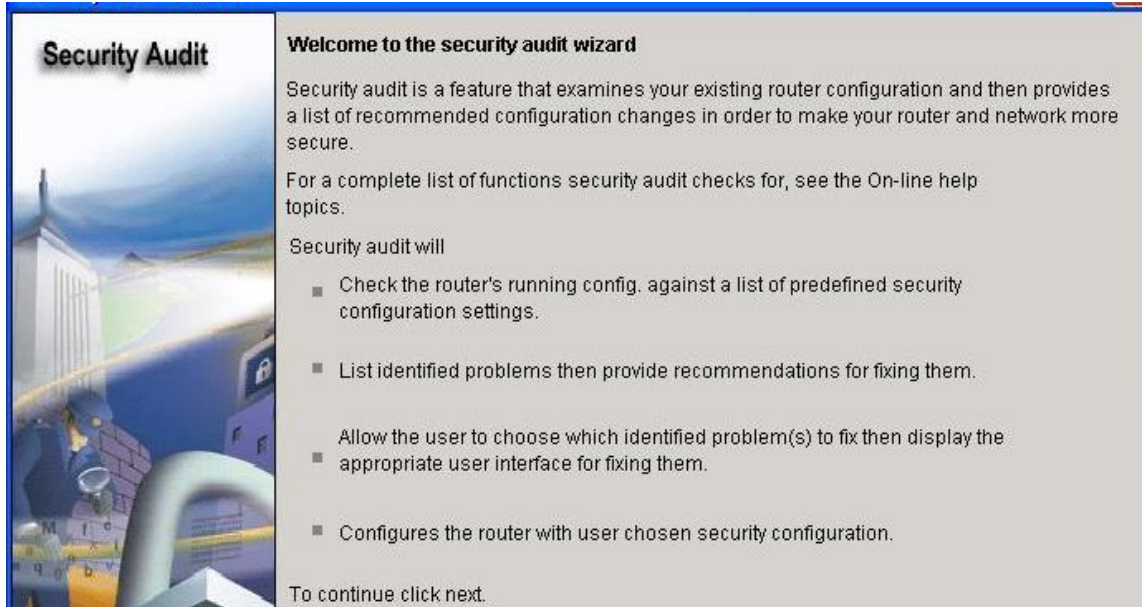


Now navigate down the left panel to **Security Audit** and click on it.



When you click on **Security Audit**, another window opens.

Step 3: Perform a Security Audit.

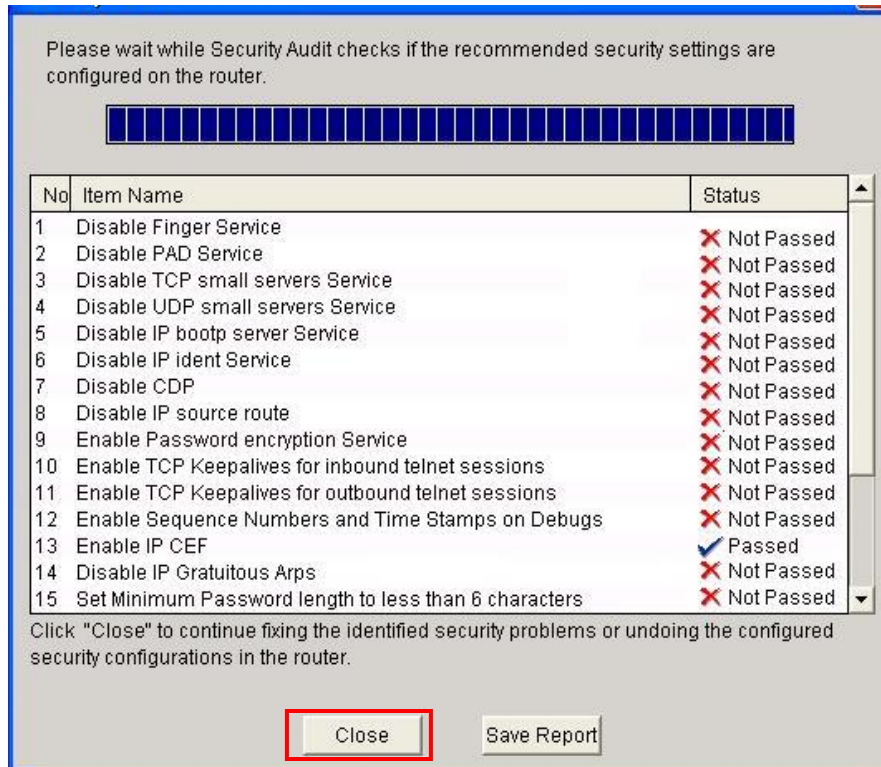


This gives a brief explanation of what the Security Audit feature does. Click on **Next** to open the Security Audit Interface configuration window.



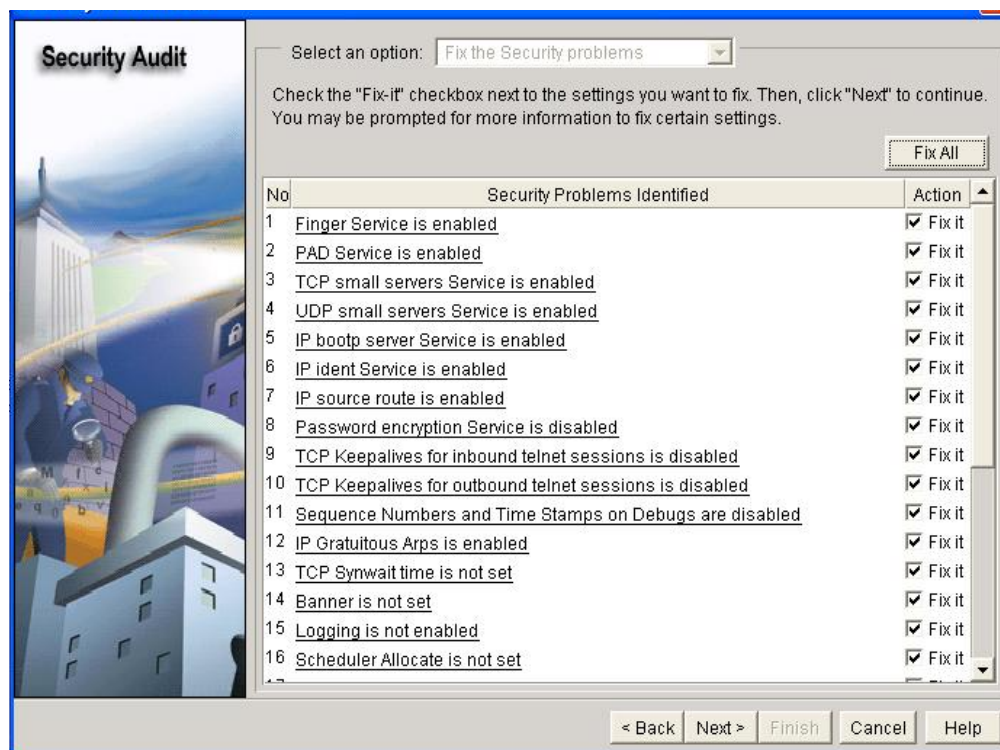
An interface should be classified as outside (untrusted) if you cannot be sure of the legitimacy of the traffic coming into the interface. In this example, both FastEthernet0/1 and Serial0/1/0 are untrusted because Serial0/1/0 is facing the Internet, and Fastethernet0/1 is facing the access part of the network and illegitimate traffic could be generated.

After selecting outside and inside interfaces, click **Next**. A new window opens indicating that SDM is conducting a security audit.

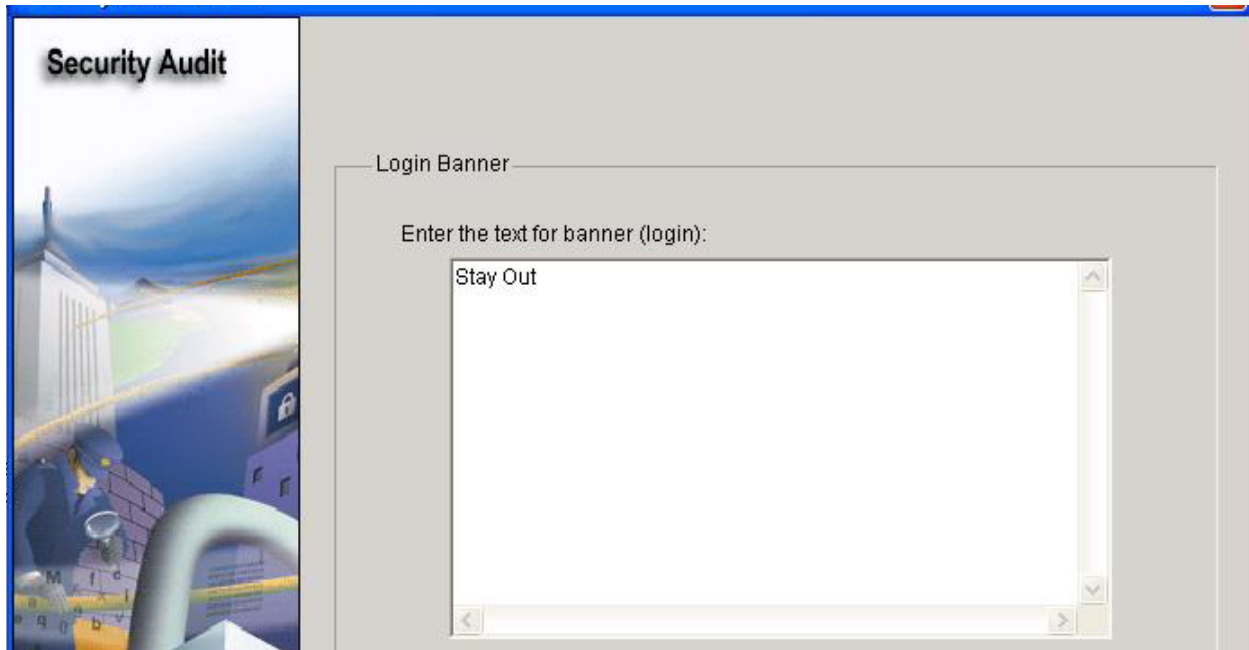


As you can see, the default configuration is insecure. Click the **Close** button to continue.

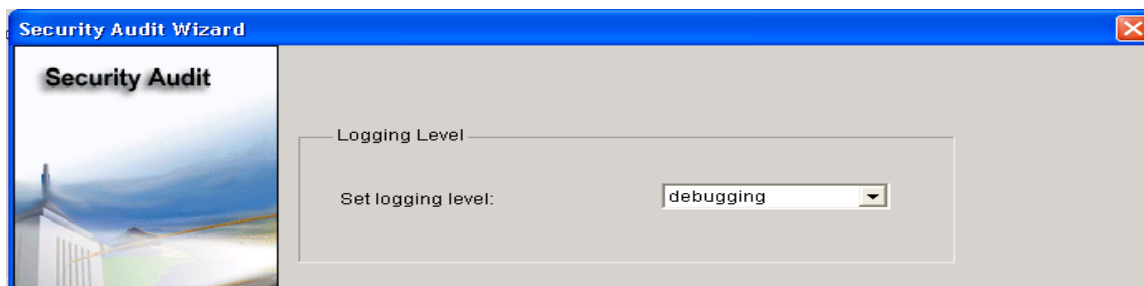
Step 4: Apply settings to the router.



Click the **Fix All** button to make all the suggested security changes. Then click the **Next** button.

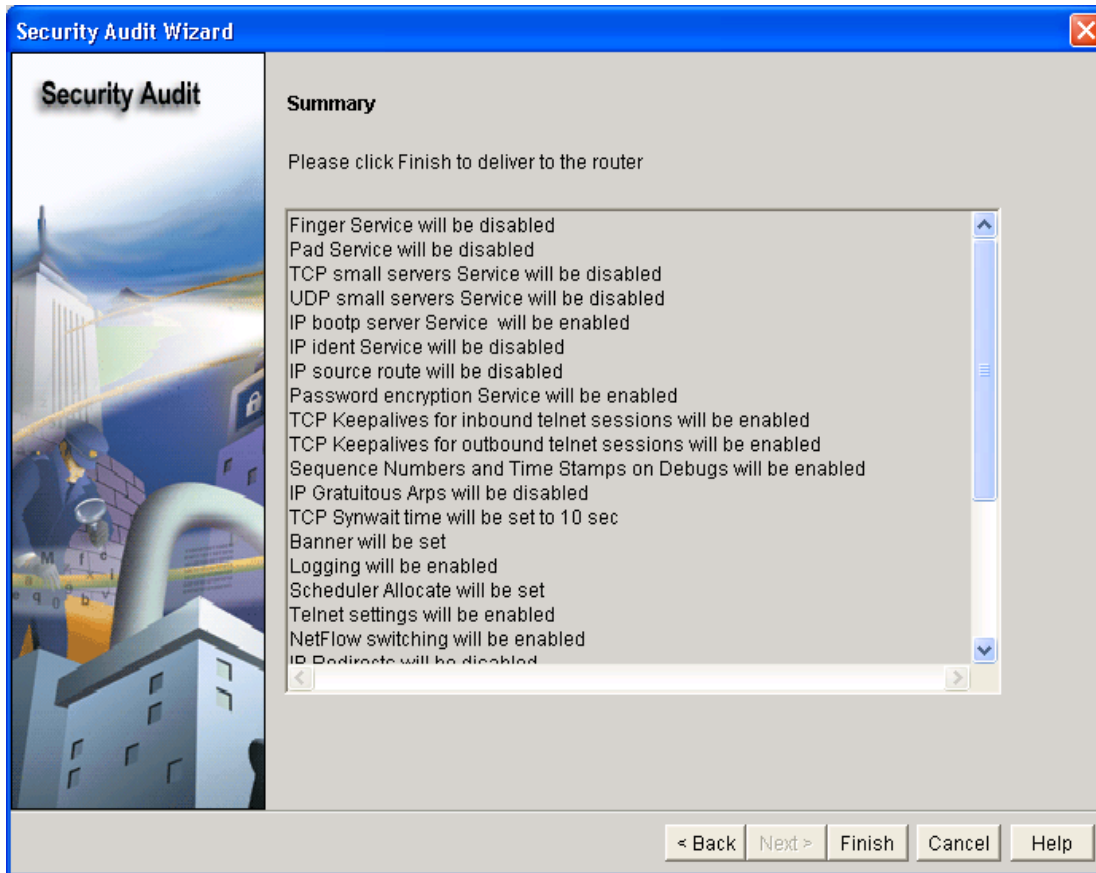


Enter a banner message to use as the message of the day for the router, and then click **Next**.

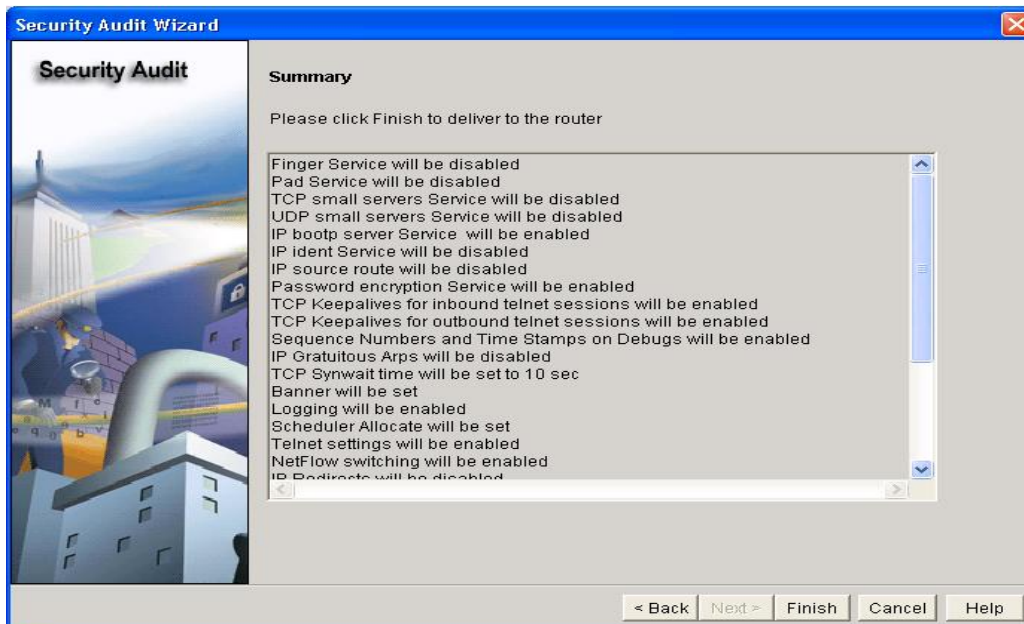


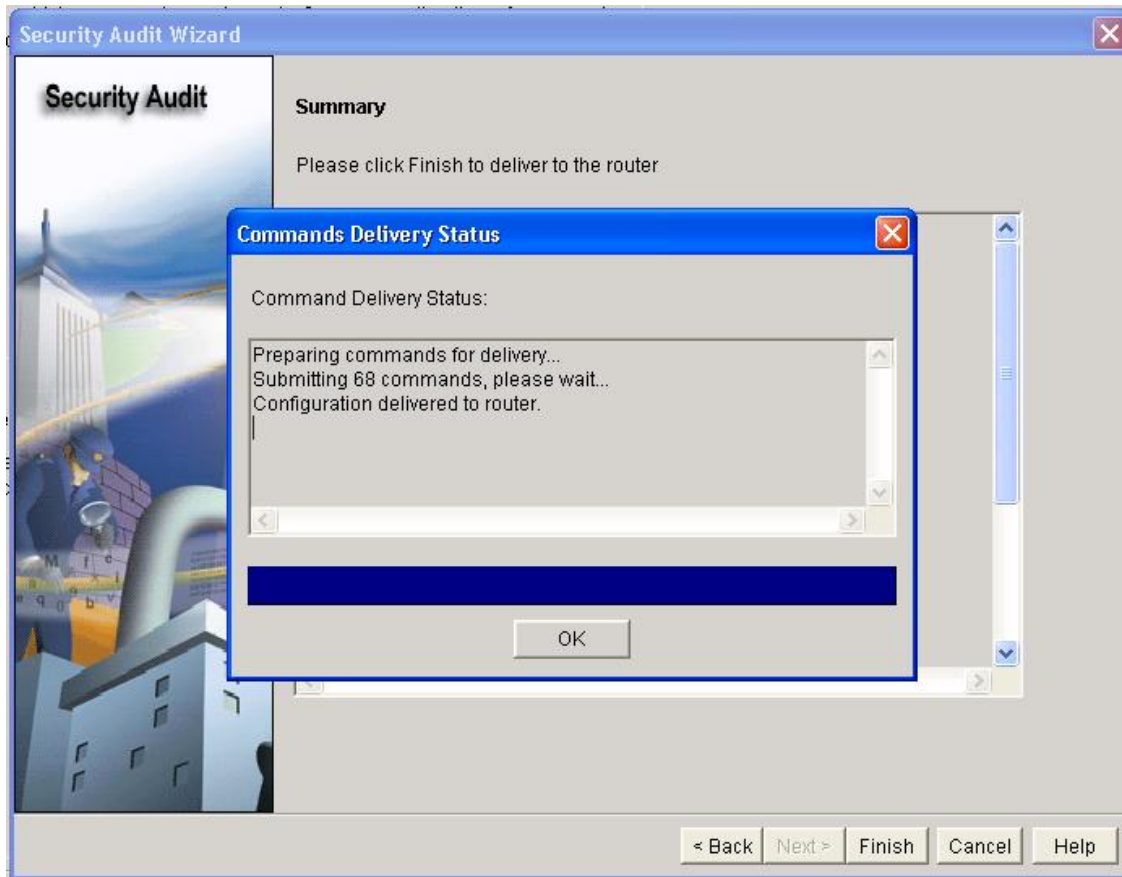
Next, set the level of severity of log traps that you want the router to send to the syslog server. The severity level is set to debugging for this scenario. Click **Next** to view a summary of the changes about to be made to the router.

Step 5: Commit the configuration to the router.



After reviewing the changes about to be committed, click **Finish**.





Click **OK** and exit SDM.

Task 9: Document the Router Configurations

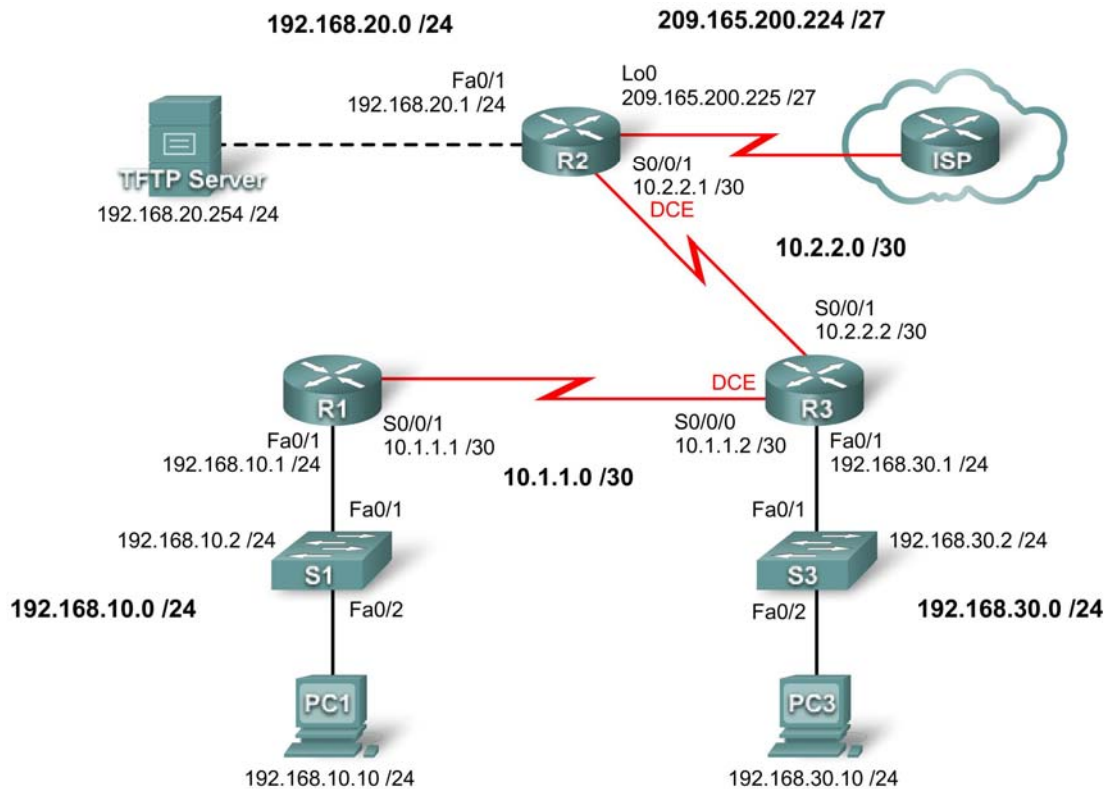
On each router, issue the **show run** command and capture the configurations.

Task 10: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 4.6.2: Challenge Security Configuration

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1	192.168.10.1	255.255.255.0	N/A
	S0/0/1	10.1.1.1	255.255.255.252	N/A
R2	Fa0/1	192.168.20.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
R3	Fa0/1	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
S1	VLAN10	192.168.10.2	255.255.255.0	N/A
S3	VLAN30	192.168.30.2	255.255.255.0	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
TFTP Server	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Perform basic configuration tasks on a router
- Configure and activate interfaces
- Configuring basic router security
- Disable unused Cisco services and interfaces
- Protect enterprise networks from basic external and internal attacks
- Understand and manage Cisco IOS configuration files and Cisco file system
- Set up and use Cisco SDM (Security Device Manager) to configure basic router security .

Scenario

In this lab, you will configure security using the network shown in the topology diagram. If you need assistance, refer to the Basic Security lab. However, try to do as much on your own as possible. For this lab, do not use password protection or login on any console lines because they might cause accidental logout. However, you should still secure the console line using other means. Use ciscocccna for all passwords in this lab.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configurations

Step 1: Configure routers.

Configure the R1, R2, and R3 routers according to the following guidelines:

- Configure the router hostname according to the topology diagram.
- Disable DNS lookup.
- Configure a message-of-the-day banner.
- Configure IP addresses on interfaces on R1, R2, and R3.
- Enable RIPv2 on all routers for all networks.
- Create a loopback interface on R2 to simulate the connection to the Internet.
- Create VLANs on switch S1 and S3 and configure the respective interfaces to participate in the VLANs
- Configure router R3 for SDM secure connectivity
- Install SDM on either PC3 or R3 if it is not installed already

Step 2: Configure Ethernet interfaces.

Configure the Ethernet interfaces of PC1, PC3, and TFTP Server with the IP addresses and default gateways from the addressing table at the beginning of the lab.

Step 3: Test the PC configuration by pinging the default gateway from each PC and the TFTP server.

Task 3: Secure Access to Routers

Step 1: Configure secure passwords and AAA authentication using a local database.

Create a secure password for router access. Create the username **ccna** to store locally on the router. Configure the router to use the local authentication database. Remember to use **ciscoccna** for all passwords in this lab.

Step 2: Secure the console the vty lines.

Configure the console and vty lines to block a user who enters an incorrect username and password five times within 2 minutes. Block additional login attempts for 2 minutes.

Step 3: Verify that connection attempts are denied after the failed attempt limit is reached.

Task 4: Secure Access to the Network

Step 1: Secure the RIP routing protocol.

Do not send RIP updates to non-network routers. Authenticate RIP updates and encrypt them.

Step 2: Verify that RIP routing still works.

Task 5: Logging Activity with SNMP (Simple Network Management Protocol)

Step 1: Configure SNMP logging to the syslog server at 192.168.10.250 on all devices.

Step 2: Log all messages with severity level 4 to the syslog server.

Task 6: Disabling Unused Cisco Network Services

Step 1: Disable unused interfaces on all devices.

Step 2: Disable unused global services on R1.

Step 3: Disable unused interface services on R1.

Step 4: Use AutoSecure to secure R2.

Remember to use **ciscoccna** for all passwords in this lab.

Task 7: Managing Cisco IOS and Configuration Files

Step 1: Identify where the running-config file is located in router memory.

Step 2: Transfer the running-config file from R1 to R2 using TFTP.

Step 3: Break R1 and recover it using ROMmon.

Copy and paste the following commands on R1, and then recover R1 using ROMmon.

```
line vty 0 4
  exec-timeout 0 20
line console 0
  exec-timeout 0 20
end
copy run start
exit
```

Step 4: Restore the saved configuration to R1 from R2 using TFTP.

Step 5: Erase the saved configuration from R2.

Task 8: Using SDM to Secure R3

Step 1: Connect to R2 using PC1.

Step 2: Navigate to the Security Audit feature.

Step 3: Perform a Security Audit.

Step 4: Choose settings to apply to the router.

Step 5: Commit the configuration to the router.

Task 9: Document the Router Configurations

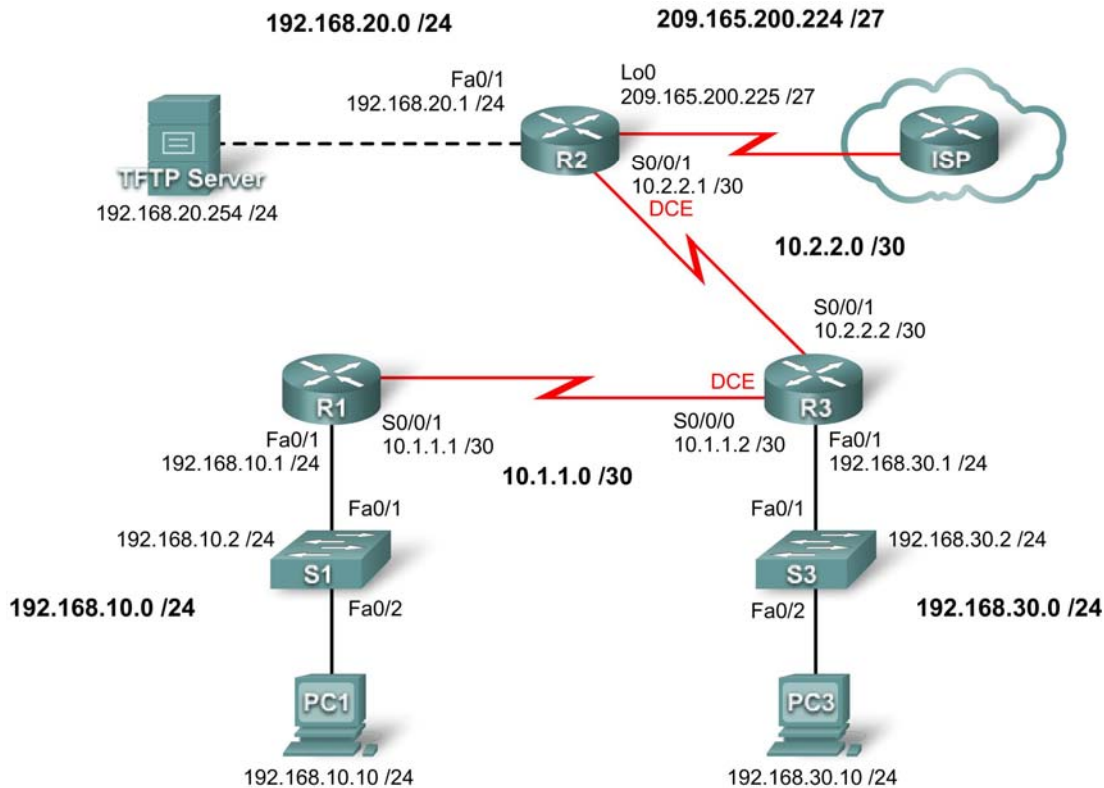
On each router, issue the **show run** command and capture the configurations.

Task 10: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 4.6.3: Troubleshooting Security Configuration

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1	192.168.10.1	255.255.255.0	N/A
	S0/0/1	10.1.1.1	255.255.255.252	N/A
R2	Fa0/1	192.168.20.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
R3	Fa0/1	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
S1	VLAN10	192.168.10.2	255.255.255.0	N/A
S3	VLAN30	192.168.30.2	255.255.255.0	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
TFTP Server	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Erase the startup configuration and restore all routers to the default state
- Load routers with supplied scripts
- Find and correct all network errors
- Document the corrected network

Scenario

Your company just hired a new network engineer who has created some security issues in the network with misconfigurations and oversights. Your boss has asked you to correct the errors the new engineer has made configuring the routers. While correcting the problems, make sure that all the devices are secure but are still accessible by administrators, and that all networks are reachable. All routers must be accessible with SDM from PC1. Verify that a device is secure by using tools such as Telnet and ping. Unauthorized use of these tools should be blocked, but also ensure that authorized use is permitted. For this lab, do not use login or password protection on any console lines to prevent accidental lockout. Use **ciscoccna** for all passwords in this scenario.

Task 1: Load Routers with the Supplied Scripts

Load the following configurations into the devices in the topology.

R1:

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 10 log
security passwords min-length 6
enable secret ciscoccna
!
aaa new-model
!
aaa authentication login LOCAL_AUTH local
!
aaa session-id common
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip source-route
no ip gratuitous-arps
```

```
ip cef
!
no ip dhcp use vrf connected
!
no ip bootp server
!
key chain RIP_KEY
  key 1
    key-string cisco
username ccna password ciscoccna
!
interface FastEthernet0/0
  no ip address
  no ip redirects
  no ip unreachables
  no ip proxy-arp
  no shutdown
  duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 192.168.10.1 255.255.255.0
  no ip redirects
  no ip unreachables
  no ip proxy-arp
  duplex auto
  speed auto
  no shutdown
!
!
interface Serial0/0/0
  no ip address
  no ip redirects
  no ip unreachables
  no ip proxy-arp
  no shutdown
  no fair-queue
  clockrate 125000
!
interface Serial0/0/1
  ip address 10.1.1.1 255.255.255.252
  no ip redirects
  no ip unreachables
  no ip proxy-arp
  no shutdown
!
interface Serial0/1/0
  no ip address
  no ip redirects
  no ip unreachables
  no ip proxy-arp
  no shutdown
  clockrate 2000000
!
interface Serial0/1/1
  no ip address
```

```
no ip redirects
no ip unreachable
no ip proxy-arp
no shutdown
!
router rip
version 2
passive-interface default
no passive-interface Serial0/0/0
network 10.0.0.0
network 192.168.10.0
no auto-summary
!
ip classless
!
no ip http server
!
logging 192.168.10.150
no cdp run
!
line con 0
exec-timeout 5 0
logging synchronous
transport output telnet
line aux 0
exec-timeout 15 0
logging synchronous
login authentication local_auth
transport output telnet
line vty 0 4
exec-timeout 5 0
logging synchronous
login authentication local_auth
!
end
```

R2:

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname R2
!
security authentication failure rate 10 log
security passwords min-length 6
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
```

```
no mmi pvc
mmi snmp-timeout 180
no ip source-route
no ip gratuitous-arps
ip cef
!
no ip dhcp use vrf connected
!
no ip bootp server
!
!
username ccna password ciscoccna
!
!
interface FastEthernet0/0
  no ip address
  no ip redirects
  no ip unreachableables
  no ip proxy-arp
  no ip directed-broadcast
  shutdown
  duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 192.168.20.1 255.255.255.0
  no ip redirects
  no ip unreachableables
  no ip proxy-arp
  no ip directed-broadcast
  duplex auto
  speed auto
  no shutdown
!
interface Serial0/0/0
  no ip address
  no ip redirects
  no ip unreachableables
  no ip proxy-arp
  no ip directed-broadcast
  shutdown
  no fair-queue
!
interface Serial0/0/1
  ip address 10.2.2.1 255.255.255.252
  no ip redirects
  no ip unreachableables
  no ip proxy-arp
  no ip directed-broadcast
  ip rip authentication mode md5
  ip rip authentication key-chain RIP_KEY
  clockrate 128000
  no shutdown
!
interface Serial0/1/0
  ip address 209.165.200.224 255.255.255.224
```

```
no ip redirects
no ip unreachable
no ip proxy-arp
no ip directed-broadcast
no shutdown
!
interface Serial0/1/1
no ip address
no ip redirects
no ip unreachable
no ip proxy-arp
no ip directed-broadcast
shutdown
clockrate 2000000
!
router rip
version 2
no passive-interface Serial0/0/1
network 10.0.0.0
network 192.168.20.0
no auto-summary
!
ip classless
!
no ip http server
!
logging trap debugging
logging 192.168.10.150
!
line con 0
exec-timeout 5 0
logging synchronous
transport output telnet
line aux 0
exec-timeout 15 0
logging synchronous
login authentication local_auth
transport output telnet
line vty 0 4
exec-timeout 0 0
logging synchronous
login authentication local_auth
transport input telnet
!
end
```

R3:

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
```

```
!  
security authentication failure rate 10 log  
security passwords min-length 6  
enable secret ciscoccna  
!  
aaa new-model  
!  
aaa authentication login local_auth local  
!  
aaa session-id common  
!  
resource policy  
!  
mmi polling-interval 60  
no mmi auto-configure  
no mmi pvc  
mmi snmp-timeout 180  
ip subnet-zero  
no ip source-route  
no ip gratuitous-arps  
ip cef  
!  
!  
no ip dhcp use vrf connected  
!  
no ip bootp server  
!  
key chain RIP_KEY  
  key 1  
    key-string Cisco  
!  
interface FastEthernet0/0  
  no ip address  
  no ip redirects  
  no ip proxy-arp  
  no ip directed-broadcast  
  duplex auto  
  speed auto  
  shutdown  
!  
interface FastEthernet0/1  
  ip address 192.168.30.1 255.255.255.0  
  no ip redirects  
  no ip unreachablees  
  no ip proxy-arp  
  no ip directed-broadcast  
  no shutdown  
  duplex auto  
  speed auto  
!  
interface Serial0/0/0  
  ip address 10.1.1.2 255.255.255.252  
  no ip redirects  
  no ip unreachablees  
  no ip proxy-arp  
  no ip directed-broadcast
```

```
clockrate 125000
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 no ip redirects
 no ip unreachable
 no ip proxy-arp
 no ip directed-broadcast
!
router rip
 version 2
 passive-interface default
 passive-interface Serial0/0/0
 passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.30.0
 no auto-summary
!
ip classless
!
no ip http server
!
logging trap debugging
logging 192.168.10.150
no cdp run
!
control-plane
!
line con 0
 exec-timeout 5 0
 logging synchronous
 transport output telnet
line aux 0
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport output telnet
line vty 0 4
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport input telnet
!
end
```

Task 2: Find and Correct all Network Errors

Using standard troubleshooting methods, find, document, and correct each error.

Note: When troubleshooting a production network that is not working, many very small mistakes can prevent everything from working correctly. The first item to check is the spelling and case of all passwords, keychain names and keys, and authentication list names. It is often a mismatch in case or spelling that causes total failure. The best practice is to start with the most basic and work upward. First ask whether all the names and keys match up. Next, if the configuration uses a list or keychain and so on, check if the item referenced actually exists and is the same on all devices. Configuring something once on one device and then copying and pasting into the other device is

the best way to ensure that the configuration is exactly the same. Next, when thinking about disabling or restricting services, ask what the services are used for and if they are needed. Also ask what information the router should be sending out. Who should and should not receive that information. Finally, ask what the services enable the users to do, and do you want them to be able to do that. Generally, if you can think of a way that a service can be abused, you should take steps to prevent that.

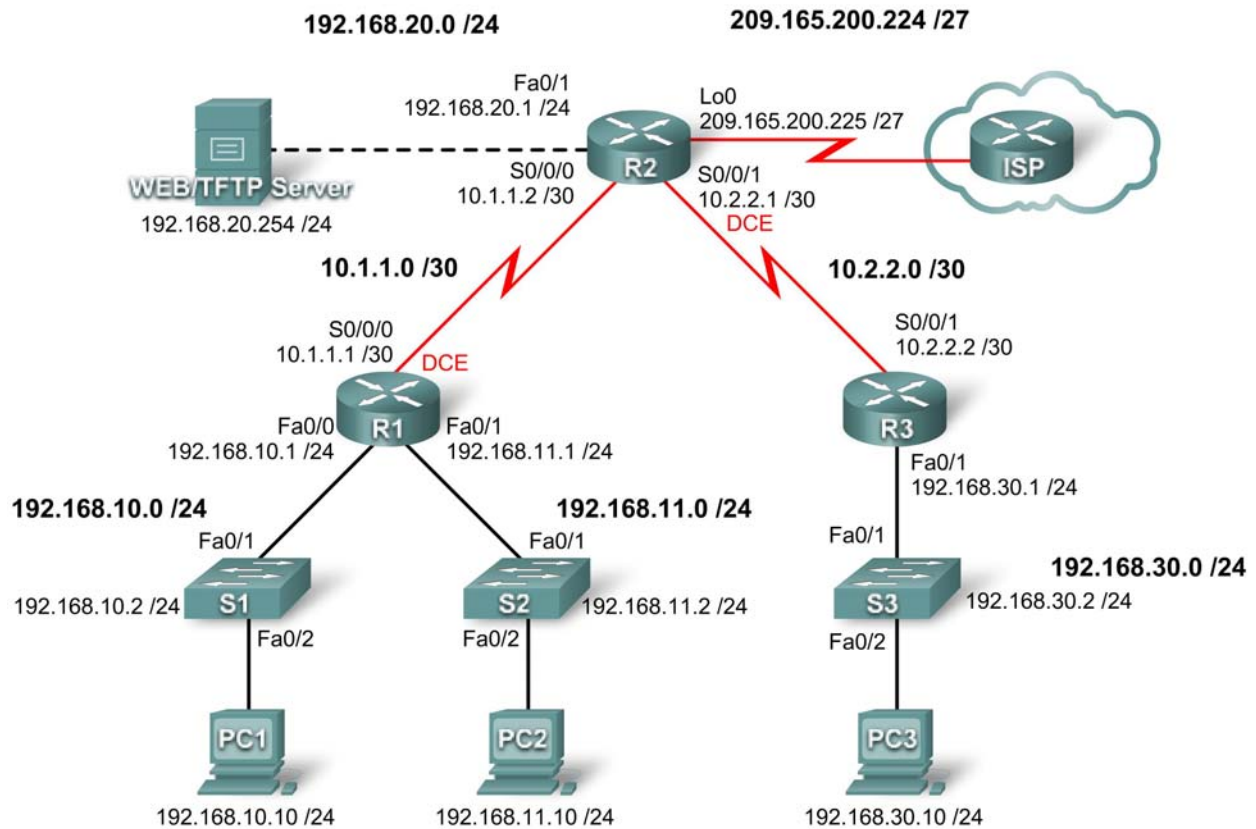
Task 3: Document the Corrected Network

Task 4: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 5.5.1: Basic Access Control Lists

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.10.1	255.255.255.0	
	Fa0/1	192.168.11.1	255.255.255.0	
	S0/0/0	10.1.1.1	255.255.255.252	
R2	Fa0/1	192.168.20.1	255.255.255.0	
	S0/0/0	10.1.1.2	255.255.255.252	
	S0/0/1	10.2.2.1	255.255.255.252	
	Lo0	209.165.200.225	255.255.255.224	
R3	Fa0/1	192.168.30.1	255.255.255.0	
	S0/0/1	10.2.2.2	255.255.255.252	
S1	Vlan1	192.168.10.2	255.255.255.0	192.168.10.1

S2	Vlan1	192.168.11.2	255.255.255.0	192.168.11.1
S3	Vlan1	192.168.30.2	255.255.255.0	192.168.30.1
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
Web Server	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Learning Objectives

Upon completion of this lab, you will be able to:

- Design named standard and named extended ACLs
- Apply named standard and named extended ACLs
- Test named standard and named extended ACLs
- Troubleshoot named standard and named extended ACLs

Scenario

In this lab, you will learn how to configure basic network security using Access Control Lists. You will apply both standard and extended ACLs.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology diagram.

Note: This lab was developed and tested using 1841 routers. If you use 1700, 2500, or 2600 series routers, the router outputs and interface descriptions might be different. On older routers, or versions of the IOS before 12.4, some commands may be different or non-existent.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configurations

Configure the R1, R2, R3, S1, S2, and S3 routers and switches according to the following guidelines:

- Configure the router hostname to match the topology diagram.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a message-of-the-day banner.
- Configure a password of cisco for console connections.
- Configure a password for VTY connections.
- Configure IP addresses and masks on all devices.
- Enable OSPF area 0 on all routers for all networks.
- Configure a loopback interface on R2 to simulate the ISP.

- Configure IP addresses for the VLAN 1 interface on each switch.
- Configure each switch with the appropriate default gateway.
- Verify full IP connectivity using the **ping** command.

Task 3: Configuring a Standard ACL

Standard ACLs can filter traffic based on source IP address only. A typical best practice is to configure a standard ACL as close to the destination as possible. In this task, you are configuring a standard ACL. The ACL is designed to block traffic from the 192.168.11.0/24 network located in a student lab from accessing any local networks on R3.

This ACL will be applied inbound on the R3 serial interface. Remember that every ACL has an implicit "deny all" that causes all traffic that has not matched a statement in the ACL to be blocked. For this reason, add the **permit any** statement to the end of the ACL.

Before configuring and applying this ACL, be sure to test connectivity from PC1 (or the Fa0/1 interface on R1) to PC3 (or the Fa0/1 interface on R3). Connectivity tests should be successful before applying the ACL.

Step 1: Create the ACL on router R3.

In global configuration mode, create a standard named ACL called **STND-1**.

```
R3(config)#ip access-list standard STND-1
```

In standard ACL configuration mode, add a statement that denies any packets with a source address of 192.168.11.0/24 and prints a message to the console for each matched packet.

```
R3(config-std-nacl)#deny 192.168.11.0 0.0.0.255 log
```

Permit all other traffic.

```
R3(config-std-nacl)#permit any
```

Step 2: Apply the ACL.

Apply the ACL **STND-1** as a filter on packets entering R3 through Serial interface 0/0/1.

```
R3(config)#interface serial 0/0/1
R3(config-if)#ip access-group STND-1 in
R3(config-if)#end
R3#copy run start
```

Step 3: Test the ACL.

Before testing the ACL, make sure that the console of R3 is visible. This will allow you to see the access list log messages when the packet is denied.

Test the ACL by pinging from PC2 to PC3. Since the ACL is designed to block traffic with source addresses from the 192.168.11.0/24 network, PC2 (192.168.11.10) should not be able to ping PC3.

You can also use an extended ping from the Fa0/1 interface on R1 to the Fa0/1 interface on R3.

```
R1#ping ip
Target IP address: 192.168.30.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.11.1
```

```
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.11.1
U.U.U
Success rate is 0 percent (0/5)
```

You should see the following message on the R3 console:

```
*Sep  4 03:22:58.935: %SEC-6-IPACCESSLOGNP: list STND-1 denied 0
0.0.0.0 -> 192.168.11.1, 1 packet
```

In privileged EXEC mode on R3, issue the **show access-lists** command. You see output similar to the following. Each line of an ACL has an associated counter showing how many packets have matched the rule.

```
Standard IP access list STND-1
 10 deny  192.168.11.0, wildcard bits 0.0.0.255 log (5 matches)
 20 permit any (25 matches)
```

The purpose of this ACL was to block hosts from the 192.168.11.0/24 network. Any other hosts, such as those on the 192.168.10.0/24 network should be allowed access to the networks on R3. Conduct another test from PC1 to PC3 to ensure that this traffic is not blocked.

You can also use an extended ping from the Fa0/0 interface on R1 to the Fa0/1 interface on R3.

```
R1#ping ip
Target IP address: 192.168.30.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.10.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/43/44 ms
```

Task 4: Configuring an Extended ACL

When greater granularity is required, you should use an extended ACL. Extended ACLs can filter traffic based on more than just source address. Extended ACLs can filter on protocol, source, and destination IP addresses, and source and destination port numbers.

An additional policy for this network states that devices from the 192.168.10.0/24 LAN are only permitted to reach internal networks. Computers on this LAN are not permitted to access the Internet. Therefore, these users must be blocked from reaching the IP address 209.165.200.225. Because this requirement

needs to enforce both source and destination, an extended ACL is needed.

In this task, you are configuring an extended ACL on R1 that blocks traffic originating from any device on the 192.168.10.0/24 network to access the 209.165.200.255 host (the simulated ISP). This ACL will be applied outbound on the R1 Serial 0/0/0 interface. A typical best practice for applying extended ACLs is to place them as close to the source as possible.

Before beginning, verify that you can ping 209.165.200.225 from PC1.

Step 1: Configure a named extended ACL.

In global configuration mode, create a named extended ACL called **EXTEND-1**.

```
R1(config)#ip access-list extended EXTEND-1
```

Notice that the router prompt changes to indicate that you are now in extended ACL configuration mode. From this prompt, add the necessary statements to block traffic from the 192.168.10.0/24 network to the host. Use the **host** keyword when defining the destination.

```
R1(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225
```

Recall that the implicit “deny all” blocks all other traffic without the additional **permit** statement. Add the **permit** statement to ensure that other traffic is not blocked.

```
R1(config-ext-nacl)#permit ip any any
```

Step 2: Apply the ACL.

With standard ACLs, the best practice is to place the ACL as close to the destination as possible. Extended ACLs are typically placed close to the source. The **EXTEND-1** ACL will be placed on the Serial interface, and will filter outbound traffic.

```
R1(config)#interface serial 0/0/0
R1(config-if)#ip access-group EXTEND-1 out log
R1(config-if)#end
R1#copy run start
```

Step 3: Test the ACL.

From PC1, ping the loopback interface on R2. These pings should fail, because all traffic from the 192.168.10.0/24 network is filtered when the destination is 209.165.200.225. If the destination is any other address, the pings should succeed. Confirm this by pinging R3 from the 192.168.10.0/24 network device.

Note: The extended ping feature on R1 cannot be used to test this ACL, since the traffic will originate within R1 and will never be tested against the ACL applied to the R1 serial interface.

You can further verify this by issuing the **show ip access-list** on R1 after pinging.

```
R1#show ip access-list
Extended IP access list EXTEND-1
 10 deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225 (4 matches)
 20 permit ip any any
```

Task 5: Control Access to the VTY Lines with a Standard ACL

It is good practice to restrict access to the router VTY lines for remote administration. An ACL can be applied to the VTY lines, allowing you to restrict access to specific hosts or networks. In this task, you will configure a standard ACL to permit hosts from two networks to access the VTY lines. All other hosts are denied.

Verify that you can telnet to R2 from both R1 and R3.

Step 1: Configure the ACL.

Configure a named standard ACL on R2 that permits traffic from 10.2.2.0/30 and 192.168.30.0/24. Deny all other traffic. Call the ACL **TASK-5**.

```
R2(config)#ip access-list standard TASK-5
R2(config-std-nacl)#permit 10.2.2.0 0.0.0.3
R2(config-std-nacl)#permit 192.168.30.0 0.0.0.255
```

Step 2: Apply the ACL.

Enter line configuration mode for VTY lines 0–4.

```
R2(config)#line vty 0 4
```

Use the **access-class** command to apply the ACL to the vty lines in the inbound direction. Note that this differs from the command used to apply ACLs to other interfaces.

```
R2(config-line)#access-class TASK-5 in
R2(config-line)#end
R2#copy run start
```

Step 3: Test the ACL

Telnet to R2 from R1. Note that R1 does not have IP addresses in the address range listed in the ACL TASK-5 permit statements. Connection attempts should fail.

```
R1# telnet 10.1.1.2
Trying 10.1.1.2 ...
% Connection refused by remote host
```

From R3, telnet to R2. You will be presented with a prompt for the VTY line password.

```
R3# telnet 10.1.1.2
Trying 10.1.1.2 ... Open
CUnauthorized access strictly prohibited, violators will be prosecuted
to the full extent of the law.

User Access Verification

Password:
```

Why do connection attempts from other networks fail even though they are not specifically listed in the ACL?

Task 6: Troubleshooting ACLs

When an ACL is improperly configured or applied to the wrong interface or in the wrong direction, network traffic may be affected in an undesirable manner.

Step 1: Remove ACL STND-1 from S0/0/1 of R3.

In an earlier task, you created and applied a named standard ACL on R3. Use the **show running-config** command to view the ACL and its placement. You should see that an ACL named **STND-1** was configured and applied inbound on Serial 0/0/1. Recall that this ACL was designed to block all network

traffic with a source address from the 192.168.11.0/24 network from accessing the LAN on R3.

To remove the ACL, go to interface configuration mode for Serial 0/0/1 on R3. Use the **no ip access-group STND-1 in** command to remove the ACL from the interface.

```
R3(config)#interface serial 0/0/1
R3(config-if)#no ip access-group STND-1 in
```

Use the **show running-config** command to confirm that the ACL has been removed from Serial 0/0/1.

Step 2: Apply ACL STND-1 on S0/0/1 outbound.

To test the importance of ACL filtering direction, reapply the **STND-1** ACL to the Serial 0/0/1 interface. This time the ACL will be filtering outbound traffic, rather than inbound traffic. Remember to use the **out** keyword when applying the ACL.

```
R3(config)#interface serial 0/0/1
R3(config-if)#ip access-group STND-1 out
```

Step 3: Test the ACL.

Test the ACL by pinging from PC2 to PC3. As an alternative, use an extended ping from R1. Notice that this time pings succeed, and the ACL counters are not incremented. Confirm this by issuing the **show ip access-list** command on R3.

Step 4: Restore the ACL to its original configuration.

Remove the ACL from the outbound direction and reapply it to the inbound direction.

```
R3(config)#interface serial 0/0/1
R3(config-if)#no ip access-group STND-1 out
R3(config-if)#ip access-group STND-1 in
```

Step 5: Apply TASK-5 to the R2 serial 0/0/0 interface inbound.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip access-group TASK-5 in
```

Step 6: Test the ACL.

Attempt to communicate to any device connected to R2 or R3 from R1 or its attached networks. Notice that all communication is blocked; however, ACL counters are not incremented. This is because of the implicit "deny all" at the end of every ACL. This deny statement will prevent all inbound traffic to serial 0/0/0 from any source other than R3. Essentially, this will cause routes from R1 to be removed from the routing table.

You should see messages similar to the following printed on the consoles of R1 and R2 (It will take some time for the OSPF neighbor relationship to go down, so be patient):

```
*Sep  4 09:51:21.757: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.11.1 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
```

Once you receive this message, issue the command **show ip route** on both R1 and R2 to see which routes have been removed from the routing table.

Remove ACL TASK-5 from the interface, and save your configurations.

```
R2(config)#interface serial 0/0/0
R2(config-if)#no ip access-group TASK-5 in
R2(config)#exit
R2#copy run start
```


Task 7: Document the Router Configurations

Configurations

Router 1

```
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 no shutdown
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 ip access-group EXTEND-1 out
 clockrate 64000
 no shutdown
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
!
ip access-list extended EXTEND-1
 deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225
 permit ip any any
!
banner motd ^CUnauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 password cisco
 login
!
```

Router 2

```
hostname R2
!
enable secret class
!
no ip domain lookup
!
```

```
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 clockrate 125000
 no shutdown
!
router ospf 1
 no auto-cost
 network 10.1.1.0 0.0.0.3 area 0
 network 10.2.2.0 0.0.0.3 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 209.165.200.224 0.0.0.31 area 0
!
ip access-list standard TASK-5
 permit 10.2.2.0 0.0.0.3
 permit 192.168.30.0 0.0.0.255
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 access-class TASK-5 in
 password cisco
 login
!
```

Router 3

```
hostname R3
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/1
 ip address 192.168.30.1 255.255.255.0
 no shutdown
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 ip access-group STND-1 out
```

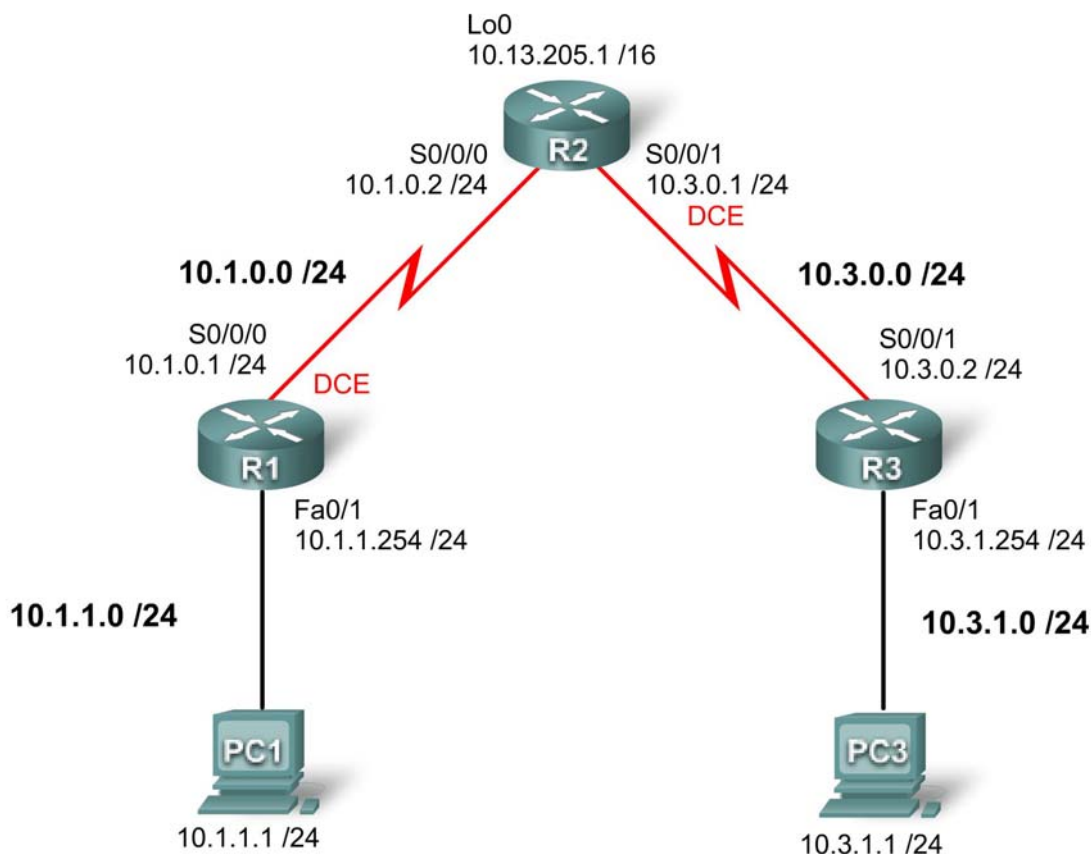
```
no shutdown
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
!
ip access-list standard STND-1
 deny 192.168.11.0 0.0.0.255 log
 permit any
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 password cisco
 login
!
end
```

Task 8: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks, such as the school LAN or the Internet, reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 5.5.2: Access Control Lists Challenge

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	S0/0/0	10.1.0.1	255.255.255.0	
	Fa0/1	10.1.1.254	255.255.255.0	
R2	S0/0/0	10.1.0.2	255.255.255.0	
	S0/0/1	10.3.0.1	255.255.255.0	
	Lo 0	10.13.205.1	255.255.0.0	
R3	S0/0/1	10.3.0.2	255.255.255.0	
	Fa0/1	10.3.1.254	255.255.255.0	
PC 1	NIC	10.1.1.1	255.255.255.0	10.1.1.254
PC 3	NIC	10.3.1.1	255.255.255.0	10.3.1.254

Learning Objectives

To complete this lab:

- Design named standard and named extended ACLs
- Apply named standard and named extended ACLs
- Test named standard and named extended ACLs
- Troubleshoot named standard and named extended ACLs

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the Topology Diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology diagram.

Note: If you use a 1700, 2500, or 2600 router, the router outputs and interface descriptions may appear different.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configurations.

Configure the R1, R2, and R3 routers according to the following guidelines:

- Configure the router hostname.
- Disable DNS lookup.
- Configure an EXEC mode password.
- Configure a message-of-the-day banner.
- Configure a password for console connections.
- Configure a password for VTY connections.
- Configure IP addresses on all devices.
- Create a loopback interface on R2.
- Enable OSPF area 0 on all routers for all networks.
- Verify full IP connectivity using the **ping** command.

Task 3: Configuring Standard ACLs

Configure standard named ACLs on the R1 and R3 VTY lines, permitting hosts connected directly to their FastEthernet subnets to gain Telnet access. Deny and log all other connection attempts. Document your testing procedures.

Task 4: Configuring Extended ACLs

Using extended ACLs on R2, complete the following requirements:

- The LANs connected to R1 and R3 are used for student computer labs. The network administrator has noticed that students in these labs are playing games across the WAN with the remote students. Make sure that your ACL prevents the LAN attached to R1 from reaching the LAN at R3 and that the LAN on R3 cannot reach the LAN on R1. Be specific in your statements so that any new LANs added to either R1 or R3 are not affected.
- Permit all OSPF traffic.
- Permit ICMP traffic to the R2 local interfaces.
- All network traffic destined to TCP port 80 should be allowed. Any other traffic should be denied and logged.
- Any traffic not specified above should be denied.

Note: This may require multiple access lists. Verify your configuration and document your testing procedure.

Why is the order of access list statements so important?

Task 5: Verifying an ACL

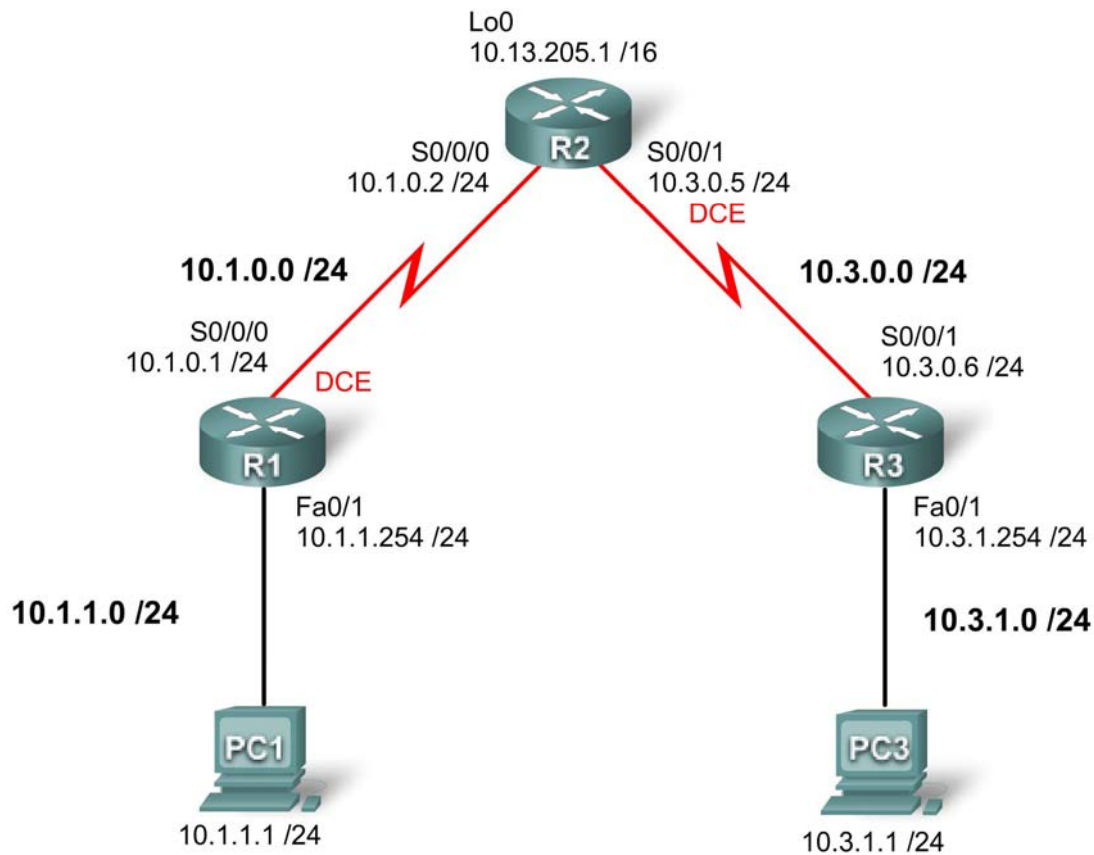
Test each protocol that you are trying block, and make sure that permitted traffic is allowed.

Task 6: Document the Router Configurations**Task 7: Clean Up**

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks, such as the school LAN or the Internet, reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 5.5.3: Troubleshooting Access Control Lists

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	S0/0/0	10.1.0.1	255.255.255.0	
	Fa0/1	10.1.1.254	255.255.255.0	
R2	S0/0/0	10.1.0.2	255.255.255.0	
	S0/0/1	10.3.0.5	255.255.255.0	
	Lo 0	10.13.205.1	255.255.0.0	
R3	S0/0/1	10.3.0.6	255.255.255.0	
	Fa0/1	10.3.1.254	255.255.255.0	

PC 1	NIC	10.1.1.1	255.255.255.0	10.1.1.254
PC 3	NIC	10.3.1.1	255.255.255.0	10.3.1.254

Learning Objectives

To complete this lab:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Load routers with scripts
- Find and correct network errors
- Document the corrected network

Scenario

You work for a regional service provider that has customers who have recently experienced several security breaches. Some security policies have been implemented that haven't addressed the specific needs of the customers. Your department has been asked to examine the configuration, conduct tests and change the configuration as necessary to secure the customer routers.

Ensure that your final configurations implement the following security policies:

- R1 and R3 customers request that only local PCs are able to access VTY lines. Log any attempts by other devices to access the VTY lines.
- R1 and R3 directly connected networks should not be allowed to send or receive traffic to each other. All other traffic should be allowed to and from R1 and R3.

A minimum of ACL statements should be used and applied inbound on the R2 serial interfaces. OSPF is used to distribute routing information. All passwords, except the enable secret password, are set to cisco. The enable secret password is set to **class**.

Task 1: Load Routers with the Supplied Scripts

Your instructor will either load the devices prior to this lab, or provide you with the configs.

Task 2: Find and Correct Network Errors

Find and correct all errors in the configuration. Document the steps you used to troubleshoot the network and note each error found.

Task 3: Document the Corrected Network

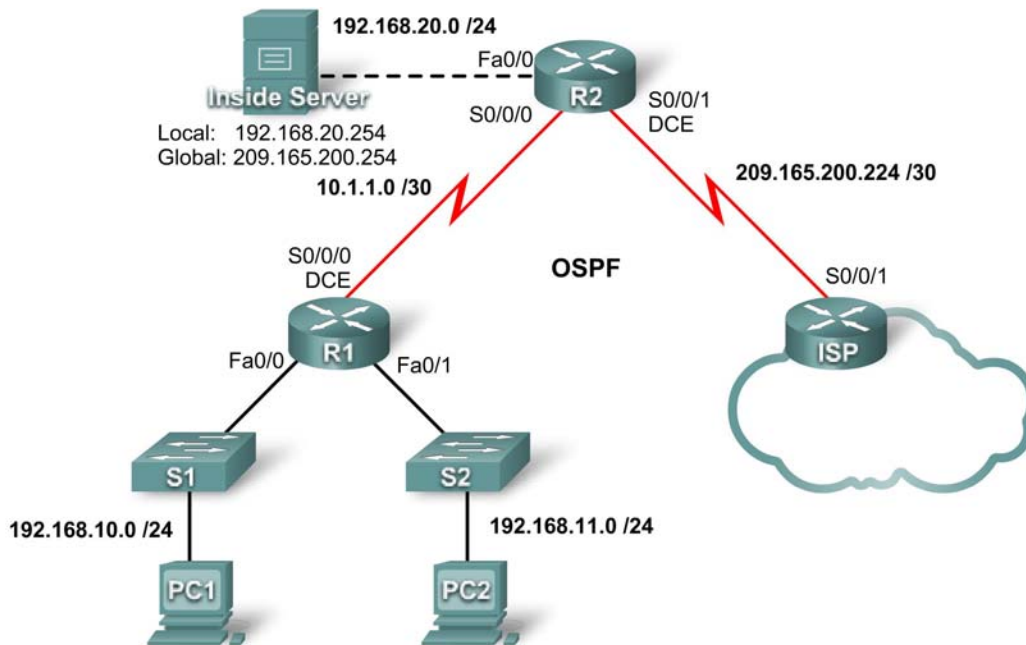
Now that you have corrected all errors and tested connectivity throughout the network, document the final configuration for each device.

Task 4: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks, such as the school LAN or the Internet, reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 7.4.1: Basic DHCP and NAT Configuration

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	S0/0/0	10.1.1.1	255.255.255.252
	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
R2	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	209.165.200.225	255.255.255.252
	Fa0/0	192.168.20.254	255.255.255.0
ISP	S0/0/1	209.165.200.226	255.255.255.252

Learning Objectives

Upon completion of this lab, you will be able to:

- Prepare the network
- Perform basic router configurations
- Configure a Cisco IOS DHCP server
- Configure static and default routing
- Configure static NAT
- Configure dynamic NAT with a pool of addresses

- Configure NAT overload

Scenario

In this lab, you will configure the DHCP and NAT IP services. One router is the DHCP server. The other router forwards DHCP requests to the server. You will also configure both static and dynamic NAT configurations, including NAT overload. When you have completed the configurations, verify the connectivity between the inside and outside addresses.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

Note: If you use a 1700, 2500, or 2600 series router, the router outputs and interface descriptions may look different. On older routers some commands may be different, or not exist.

Step 2: Clear all existing configurations on the routers.

Task 2: Perform Basic Router Configurations

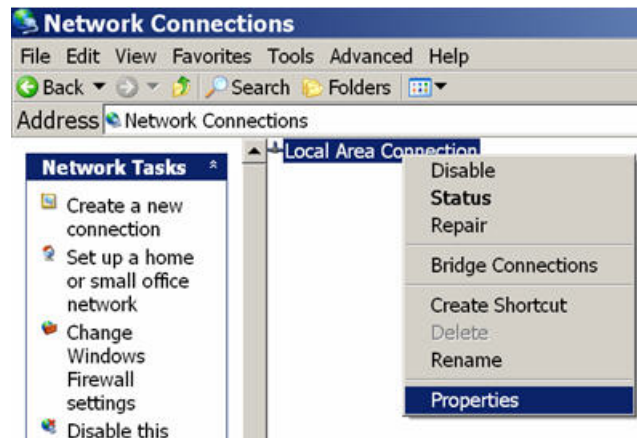
Configure the R1, R2, and ISP routers according to the following guidelines:

- Configure the device hostname.
- Disable DNS lookup.
- Configure a privileged EXEC mode password.
- Configure a message-of-the-day banner.
- Configure a password for the console connections.
- Configure a password for all vty connections.
- Configure IP addresses on all routers. The PCs receive IP addressing from DHCP later in the lab.
- Enable OSPF with process ID 1 on R1 and R2. Do not advertise the 209.165.200.224/27 network.

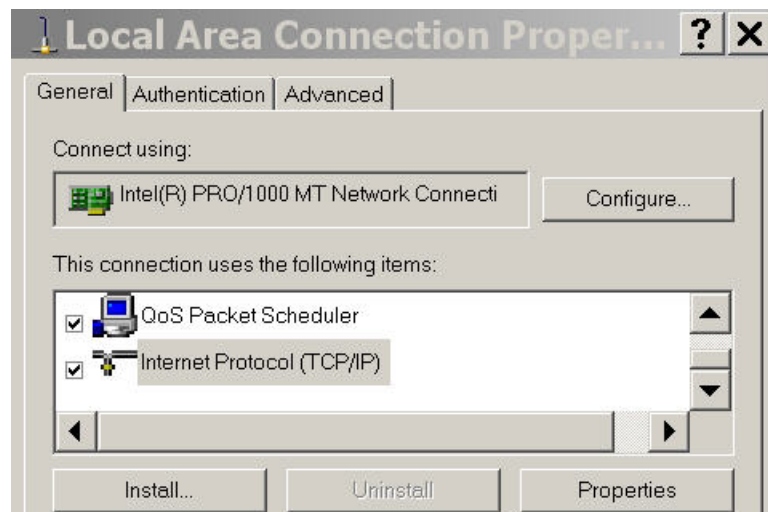
Note: Instead of attaching a server to R2, you can configure a loopback interface on R2 to use the IP address 192.168.20.254/24. If you do this, you do not need to configure the Fast Ethernet interface.

Task 3: Configure PC1 and PC2 to receive an IP address through DHCP

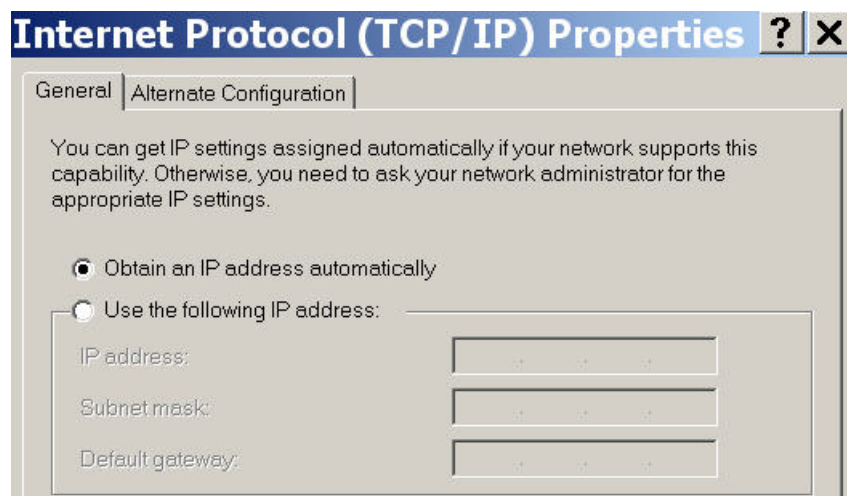
On a Windows PC go to **Start -> Control Panel -> Network Connections -> Local Area Connection**. Right mouse click on the **Local Area Connection** and select **Properties**.



Scroll down and highlight **Internet Protocol (TCP/IP)**. Click on the **Properties** button.



Make sure the button is selected that says **Obtain an IP address automatically**.



Once this has been done on both PC1 and PC2, they are ready to receive an IP address from a DHCP server.

Task 4: Configure a Cisco IOS DHCP Server

Cisco IOS software supports a DHCP server configuration called Easy IP. The goal for this lab is to have devices on the networks 192.168.10.0/24 and 192.168.11.0/24 request IP addresses via DHCP from R2.

Step 1: Exclude statically assigned addresses.

The DHCP server assumes that all IP addresses in a DHCP address pool subnet are available for assigning to DHCP clients. You must specify the IP addresses that the DHCP server should not assign to clients. These IP addresses are usually static addresses reserved for the router interface, switch management IP address, servers, and local network printer. The **ip dhcp excluded-address** command prevents the router from assigning IP addresses within the configured range. The following commands exclude the first 10 IP addresses from each pool for the LANs attached to R1. These addresses will not be assigned to any DHCP clients.

```
R2(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
R2(config)#ip dhcp excluded-address 192.168.11.1 192.168.11.10
```

Step 2: Configure the pool.

Create the DHCP pool using the **ip dhcp pool** command and name it **R1Fa0**.

```
R2(config)#ip dhcp pool R1Fa0
```

Specify the subnet to use when assigning IP addresses. DHCP pools automatically associate with an interface based on the network statement. The router now acts as a DHCP server, handing out addresses in the 192.168.10.0/24 subnet starting with 192.168.10.1.

```
R2(dhcp-config)#network 192.168.10.0 255.255.255.0
```

Configure the default router and domain name server for the network. Clients receive these settings via DHCP, along with an IP address.

```
R2(dhcp-config)#dns-server 192.168.11.5
R2(dhcp-config)#default-router 192.168.10.1
```

Note: There is not a DNS server at 192.168.11.5. You are configuring the command for practice only.

Because devices from the network 192.168.11.0/24 also request addresses from R2, a separate pool must be created to serve devices on that network. The commands are similar to the commands shown above:

```
R2(config)#ip dhcp pool R1Fa1
R2(dhcp-config)#network 192.168.11.0 255.255.255.0
R2(dhcp-config)#dns-server 192.168.11.5
R2(dhcp-config)#default-router 192.168.11.1
```

Step 3: Test DHCP

On PC1 and PC2 test whether each has received an IP address automatically. On each PC go to **Start -> Run -> cmd -> ipconfig**



What are the results of your test? _____

Why are these the results? _____

Step 4: Configure a helper address.

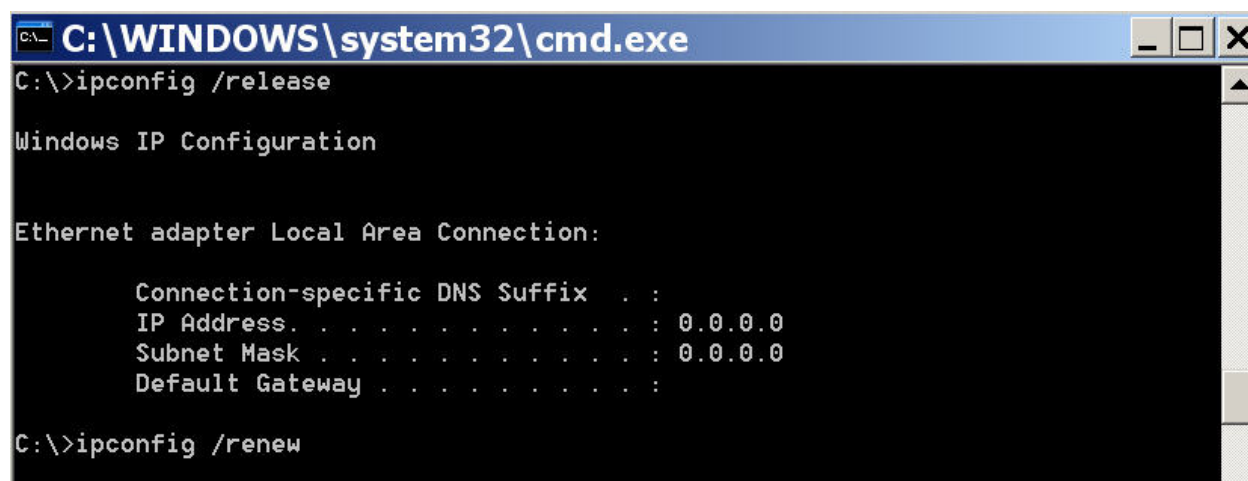
Network services such as DHCP rely on Layer 2 broadcasts to function. When the devices providing these services exist on a different subnet than the clients, they cannot receive the broadcast packets. Because the DHCP server and the DHCP clients are not on the same subnet, configure R1 to forward DHCP broadcasts to R2, which is the DHCP server, using the **ip helper-address** interface configuration command.

Notice that **ip helper-address** must be configured on each interface involved.

```
R1(config)#interface fa0/0
R1(config-if)#ip helper-address 10.1.1.2
R1(config)#interface fa0/1
R1(config-if)#ip helper-address 10.1.1.2
```

Step 5: Release and Renew the IP addresses on PC1 and PC2

Depending upon whether your PCs have been used in a different lab, or connected to the internet, they may already have learned an IP address automatically from a different DHCP server. We need to clear this IP address using the **ipconfig /release** and **ipconfig /renew** commands.



```
C:\WINDOWS\system32\cmd.exe
C:\>ipconfig /release

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : 
    IP Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 

C:\>ipconfig /renew
```

Step 6: Verify the DHCP configuration.

You can verify the DHCP server configuration in several different ways. Issue the command **ipconfig** on PC1 and PC2 to verify that they have now received an IP address dynamically. You can then issue commands on the router to get more information. The **show ip dhcp binding** command provides information on all currently assigned DHCP addresses. For instance, the following output shows that the IP address 192.168.10.11 has been assigned to MAC address 3031.632e.3537.6563. The IP lease expires on September 14, 2007 at 7:33 p.m.

```
R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/      Lease expiration      Type
                Hardware address/
                User name
192.168.10.11   0063.6973.636f.2d30.  Sep 14 2007 07:33 PM  Automatic
                3031.632e.3537.6563.
                2e30.3634.302d.566c.
```

31

The **show ip dhcp pool** command displays information on all currently configured DHCP pools on the router. In this output, the pool **R1Fa0** is configured on R1. One address has been leased from this pool. The next client to request an address will receive 192.168.10.12.

```
R2#show ip dhcp pool
```

```
Pool R1Fa0 :
  Utilization mark (high/low)      : 100 / 0
  Subnet size (first/next)          : 0 / 0
  Total addresses                    : 254
  Leased addresses                   : 1
  Pending event                     : none
  1 subnet is currently in the pool :
  Current index      IP address range      Leased addresses
  192.168.10.12      192.168.10.1 - 192.168.10.254      1
```

The **debug ip dhcp server events** command can be extremely useful when troubleshooting DHCP leases with a Cisco IOS DHCP server. The following is the debug output on R1 after connecting a host. Notice that the highlighted portion shows DHCP giving the client an address of 192.168.10.12 and mask of 255.255.255.0

```
*Sep 13 21:04:18.072: DHCPD: Sending notification of DISCOVER:
*Sep 13 21:04:18.072:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:   DHCPD: remote id 020a0000c0a80b01010000000000
*Sep 13 21:04:18.072:   DHCPD: circuit id 00000000
*Sep 13 21:04:18.072: DHCPD: Seeing if there is an internally specified pool
class:
*Sep 13 21:04:18.072:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:   DHCPD: remote id 020a0000c0a80b01010000000000
*Sep 13 21:04:18.072:   DHCPD: circuit id 00000000
*Sep 13 21:04:18.072: DHCPD: there is no address pool for 192.168.11.1.
*Sep 13 21:04:18.072: DHCPD: Sending notification of DISCOVER:
R1#
*Sep 13 21:04:18.072:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:   DHCPD: remote id 020a0000c0a80a01000000000000
*Sep 13 21:04:18.072:   DHCPD: circuit id 00000000
*Sep 13 21:04:18.072: DHCPD: Seeing if there is an internally specified pool
class:
*Sep 13 21:04:18.072:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:   DHCPD: remote id 020a0000c0a80a01000000000000
*Sep 13 21:04:18.072:   DHCPD: circuit id 00000000
R1#
*Sep 13 21:04:20.072: DHCPD: Adding binding to radix tree (192.168.10.12)
*Sep 13 21:04:20.072: DHCPD: Adding binding to hash tree
*Sep 13 21:04:20.072: DHCPD: assigned IP address 192.168.10.12 to client
0063.6973.636f.2d30.3031.632e.3537.6563.2e30.3634.302d.566c.31.
*Sep 13 21:04:20.072: DHCPD: Sending notification of ASSIGNMENT:
*Sep 13 21:04:20.072:   DHCPD: address 192.168.10.12 mask 255.255.255.0
*Sep 13 21:04:20.072:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:20.072:   DHCPD: lease time remaining (secs) = 86400
*Sep 13 21:04:20.076: DHCPD: Sending notification of ASSIGNMENT:
*Sep 13 21:04:20.076:   DHCPD: address 192.168.10.12 mask 255.255.255.0
R1#
*Sep 13 21:04:20.076:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:20.076:   DHCPD: lease time remaining (secs) = 86400
```

Task 5: Configure Static and Default Routing

ISP uses static routing to reach all networks beyond R2. However, R2 translates private addresses into public addresses before sending traffic to ISP. Therefore, ISP must be configured with the public addresses that are part of the NAT configuration on R2. Enter the following static route on ISP:

```
ISP(config)#ip route 209.165.200.240 255.255.255.240 serial 0/0/1
```

This static route includes all addresses assigned to R2 for public use.

Configure a default route on R2 and propagate the route in OSPF.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.226
R2(config)#router ospf 1
R2(config-router)#default-information originate
```

Allow a few seconds for R1 to learn the default route from R2 and then check the R1 routing table. Alternatively, you can clear the routing table with the **clear ip route *** command. A default route pointing to R2 should appear in the R1 routing table. From R1, ping the serial 0/0/1 interface on ISP (209.165.200.226). The pings should be successful. Troubleshoot if the pings fail.

Task 6: Configure Static NAT

Step 1: Statically map a public IP address to a private IP address.

The inside server attached to R2 is accessible by outside hosts beyond ISP. Statically assign the public IP address 209.165.200.254 as the address for NAT to use to map packets to the private IP address of the inside server at 192.168.20.254.

```
R2(config)#ip nat inside source static 192.168.20.254 209.165.200.254
```

Step 2: Specify inside and outside NAT interfaces.

Before NAT can work, you must specify which interfaces are inside and which interfaces are outside.

```
R2(config)#interface serial 0/0/1
R2(config-if)#ip nat outside
R2(config-if)#interface fa0/0
R2(config-if)#ip nat inside
```

Note: If using a simulated inside server, assign the **ip nat inside** command to the loopback interface.

Step 3: Verify the static NAT configuration.

From ISP, ping the public IP address 209.165.200.254.

Task 7: Configure Dynamic NAT with a Pool of Addresses

While static NAT provides a permanent mapping between an internal address and a specific public address, dynamic NAT maps private IP addresses to public addresses. These public IP addresses come from a NAT pool.

Step 1: Define a pool of global addresses.

Create a pool of addresses to which matched source addresses are translated. The following command creates a pool named MY-NAT-POOL that translates matched addresses to an available IP address in the 209.165.200.241–209.165.200.246 range.

```
R2(config)#ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask
255.255.255.248
```


Step 2: Create an extended access control list to identify which inside addresses are translated.

```
R2(config)#ip access-list extended NAT
R2(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 any
R2(config-ext-nacl)#permit ip 192.168.11.0 0.0.0.255 any
```

Step 3: Establish dynamic source translation by binding the pool with the access control list.

A router can have more than one NAT pool and more than one ACL. The following command tells the router which address pool to use to translate hosts that are allowed by the ACL.

```
R2(config)#ip nat inside source list NAT pool MY-NAT-POOL
```

Step 4: Specify inside and outside NAT interfaces.

You have already specified the inside and outside interfaces for your static NAT configuration. Now add the serial interface linked to R1 as an inside interface.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip nat inside
```

Step 5: Verify the configuration.

Ping ISP from PC1 or the Fast Ethernet interface on R1 using extended **ping**. Then use the **show ip nat translations** and **show ip nat statistics** commands on R2 to verify NAT.

```
R2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.241:4 192.168.10.1:4    209.165.200.226:4 209.165.200.226:4
--- 209.165.200.241    192.168.10.1     ---               ---
--- 209.165.200.254    192.168.20.254   ---               ---
```

```
R2#show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 0 extended)
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0, Loopback0
Hits: 23 Misses: 3
CEF Translated packets: 18, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:
-- Inside Source
[Id: 1] access-list NAT pool MY-NAT-POOL refcount 1
  pool MY-NAT-POOL: netmask 255.255.255.248
    start 209.165.200.241 end 209.165.200.246
    type generic, total addresses 6, allocated 1 (16%), misses 0
Queued Packets: 0
```

To troubleshoot issues with NAT, you can use the **debug ip nat** command. Turn on NAT debugging and repeat the ping from PC1.

```
R2#debug ip nat
IP NAT debugging is on
R2#
*Sep 13 21:15:02.215: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [25]
*Sep 13 21:15:02.231: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [25]
*Sep 13 21:15:02.247: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [26]
*Sep 13 21:15:02.263: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [26]
```

```
*Sep 13 21:15:02.275: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [27]
*Sep 13 21:15:02.291: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [27]
*Sep 13 21:15:02.307: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [28]
*Sep 13 21:15:02.323: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [28]
*Sep 13 21:15:02.335: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [29]
*Sep 13 21:15:02.351: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [29]
R2#
```

Task 8: Configure NAT Overload

In the previous example, what would happen if you needed more than the six public IP addresses that the pool allows?

By tracking port numbers, NAT overloading allows multiple inside users to reuse a public IP address.

In this task, you will remove the pool and mapping statement configured in the previous task. Then you will configure NAT overload on R2 so that all internal IP addresses are translated to the R2 S0/0/1 address when connecting to any outside device.

Step 1: Remove the NAT pool and mapping statement.

Use the following commands to remove the NAT pool and the map to the NAT ACL.

```
R2(config)#no ip nat inside source list NAT pool MY-NAT-POOL
R2(config)#no ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask
255.255.255.248
```

If you receive the following message, clear your NAT translations.

```
%Pool MY-NAT-POOL in use, cannot destroy
R2#clear ip nat translation *
```

Step 2: Configure PAT on R2 using the serial 0/0/1 interface public IP address.

The configuration is similar to dynamic NAT, except that instead of a pool of addresses, the **interface** keyword is used to identify the outside IP address. Therefore, no NAT pool is defined. The **overload** keyword enables the addition of the port number to the translation.

Because you already configured an ACL to identify which inside IP addresses to translate as well as which interfaces are inside and outside, you only need to configure the following:

```
R2(config)#ip nat inside source list NAT interface S0/0/1 overload
```

Step 3: Verify the configuration.

Ping ISP from PC1 or the Fast Ethernet interface on R1 using extended **ping**. Then use the **show ip nat translations** and **show ip nat statistics** commands on R2 to verify NAT.

```
R2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.225:6 192.168.10.11:6   209.165.200.226:6 209.165.200.226:6
--- 209.165.200.254    192.168.20.254    ---                ---
```

```
R2#show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Outside interfaces:
  Serial0/0/1
Inside interfaces:
```

```

Serial0/0/0, Loopback0
Hits: 48 Misses: 6
CEF Translated packets: 46, CEF Punted packets: 0
Expired translations: 5
Dynamic mappings:
-- Inside Source
[Id: 2] access-list NAT interface Serial0/0/1 refcount 1
Queued Packets: 0

```

Note: In the previous task, you could have added the keyword **overload** to the **ip nat inside source list NAT pool MY-NAT-POOL** command to allow for more than six concurrent users.

Task 9: Document the Network

On each router, issue the **show run** command and capture the configurations.

```

R1#show run
<output omitted>
!
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
ip address 192.168.10.1 255.255.255.0
ip helper-address 10.1.1.2
no shutdown
!
interface FastEthernet0/1
ip address 192.168.11.1 255.255.255.0
ip helper-address 10.1.1.2
no shutdown
!
interface Serial0/0/0
ip address 10.1.1.1 255.255.255.252
clock rate 125000
!
interface Serial0/0/1
no ip address
shutdown
!
router ospf 1
network 10.1.1.0 0.0.0.3 area 0
network 192.168.10.0 0.0.0.255 area 0
network 192.168.11.0 0.0.0.255 area 0
!
!
banner motd ^C
*****
!!!AUTHORIZED ACCESS ONLY!!!
*****
^C
!
line con 0

```

```
exec-timeout 0 0
password cisco
logging synchronous
login
line aux 0
exec-timeout 0 0
password cisco
logging synchronous
login
line vty 0 4
exec-timeout 0 0
password cisco
logging synchronous
login
!
end
```

R2#show run

```
!
hostname R2
!
!
enable secret class
!
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp excluded-address 192.168.11.1 192.168.11.10
!
ip dhcp pool R1Fa0
  network 192.168.10.0 255.255.255.0
  default-router 192.168.10.1
  dns-server 192.168.11.5
!
ip dhcp pool R1Fa1
  network 192.168.11.0 255.255.255.0
  dns-server 192.168.11.5
  default-router 192.168.11.1
!
no ip domain lookup
!
interface Loopback0
ip address 192.168.20.254 255.255.255.0
ip nat inside
ip virtual-reassembly
!
!
!
interface Serial0/0/0
ip address 10.1.1.2 255.255.255.252
ip nat inside
ip virtual-reassembly
!
interface Serial0/0/1
ip address 209.165.200.225 255.255.255.252
ip nat outside
ip virtual-reassembly
```

```
clock rate 125000
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.20.0 0.0.0.255 area 0
 default-information originate
!
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
!
no ip http server
no ip http secure-server
ip nat inside source list NAT interface Serial0/0/1 overload
ip nat inside source static 192.168.20.254 209.165.200.254
!
ip access-list extended NAT
 permit ip 192.168.10.0 0.0.0.255 any
 permit ip 192.168.11.0 0.0.0.255 any
!
!
banner motd ^C
*****
!!!AUTHORIZED ACCESS ONLY!!!
*****
^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
!
end
```

```
ISP#show run
<output omitted>
!
hostname ISP
!
enable secret class
!
no ip domain lookup
!
interface Serial0/0/1
```

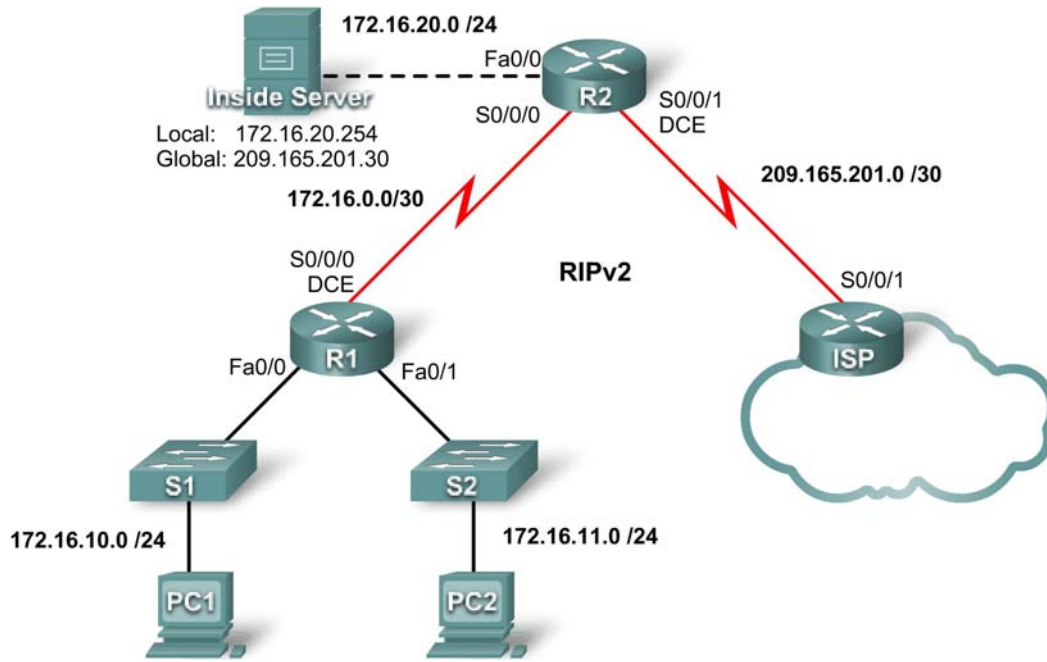
```
ip address 209.165.200.226 255.255.255.252
no shutdown
!
!
!
ip route 209.165.200.240 255.255.255.240 Serial0/0/1
!
banner motd ^C
*****
!!!AUTHORIZED ACCESS ONLY!!!
*****
^C
!
line con 0
exec-timeout 0 0
password cisco
logging synchronous
login
line aux 0
exec-timeout 0 0
password cisco
logging synchronous
login
line vty 0 4
password cisco
logging synchronous
login
!
end
```

Task 10: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks, such as the school LAN or the Internet, reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 7.4.2: Challenge DHCP and NAT Configuration

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	S0/0/0	172.16.0.1	255.255.255.252
	Fa0/0	172.16.10.1	255.255.255.0
	Fa0/1	172.16.11.1	255.255.255.0
R2	S0/0/0	172.16.0.2	255.255.255.252
	S0/0/1	209.165.201.1	255.255.255.252
	Fa0/0	172.16.20.1	255.255.255.0
ISP	S0/0/1	209.165.201.2	255.255.255.252

Learning Objectives

Upon completion of this lab, you will be able to:

- Prepare the network
- Perform basic router configurations
- Configure a Cisco IOS DHCP server
- Configure static and default routing
- Configure static NAT

- Configure dynamic NAT with a pool of addresses
- Configure NAT overload

Scenario

In this lab, configure the IP address services using the network shown in the topology diagram. If you need assistance, refer back to the basic DHCP and NAT configuration lab. However, try to do as much on your own as possible.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

Note: If you use a 1700, 2500, or 2600 series router, the router outputs and interface descriptions may look different.

Step 2: Clear all existing configurations on the routers.

Task 2: Perform Basic Router Configurations

Configure the R1, R2, and ISP routers according to the following guidelines:

- Configure the device hostname.
- Disable DNS lookup.
- Configure a privileged EXEC mode password.
- Configure a message-of-the-day banner.
- Configure a password for the console connections.
- Configure a password for all vty connections.
- Configure IP addresses on all routers. The PCs receive IP addressing from DHCP later in the lab.
- Enable OSPF with process ID 1 on R1 and R2. Do not advertise the 209.165.200.224/27 network.

Note: Instead of attaching a server to R2, you can configure a loopback interface on R2 to use the IP address 192.168.20.254/24. If you do this, you do not need to configure the Fast Ethernet interface.

Task 3: Configure a Cisco IOS DHCP Server

Configure R2 as the DHCP server for the two R1 LANs.

Step 1: Exclude statically assigned addresses.

Exclude the first three addresses from each pool.

Step 2: Configure the DHCP pool.

Create two DHCP pools. Name one of them **R1_LAN10** for the 172.16.10.0/24 network, and name the other **R1_LAN11** for the 172.16.11.0/24 network.

Configure each pool with a default gateway and a simulated DNS at 172.16.20.254.

Step 3: Configure a helper address.

Configure helper addresses so that broadcasts from client broadcasts are forwarded to the DHCP server.

Step 4: Verify the DHCP configuration.

Task 4: Configure Static and Default Routing

Configure ISP with a static route for the 209.165.201.0/27 network. Use the exit interface as an argument.

Configure a default route on R2 and propagate the route in OSPF. Use the next-hop IP address as an argument.

Task 5: Configure Static NAT

Step 1: Statically map a public IP address to a private IP address.

Statically map the inside server IP address to the public address 209.165.201.30.

Step 2: Specify inside and outside NAT interfaces.

Step 3: Verify the static NAT configuration.

Task 6: Configure Dynamic NAT with a Pool of Addresses

Step 1: Define a pool of global addresses.

Create a pool named **NAT_POOL** for the IP addresses 209.165.201.9 through 209.165.201.14 using a /29 subnet mask.

Step 2: Create a standard named access control list to identify which inside addresses are translated.

Use the name **NAT_ACL** and allow all hosts attached to the two LANs on R1.

Step 3: Establish dynamic source translation.

Bind the NAT pool to the ACL and allow NAT overloading.

Step 4: Specify the inside and outside NAT interfaces.

Verify that the inside and outside interfaces are all correctly specified.

Step 5: Verify the configuration.

Task 7: Document the Network

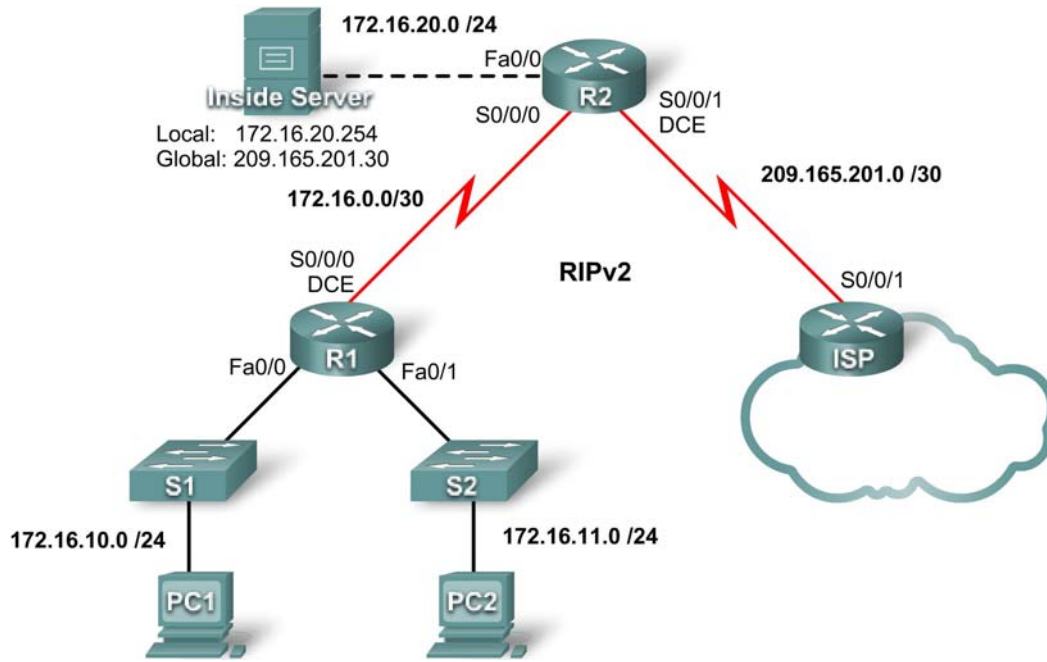
On each router, issue the **show run** command and capture the configurations.

Task 8: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks, such as the school LAN or the Internet, reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 7.4.3: Troubleshooting DHCP and NAT

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	S0/0/0	172.16.0.1	255.255.255.252
	Fa0/0	172.16.10.1	255.255.255.0
	Fa0/1	172.16.11.1	255.255.255.0
R2	S0/0/0	172.16.0.2	255.255.255.252
	S0/0/1	209.165.201.1	255.255.255.252
	Fa0/0	172.16.20.1	255.255.255.0
ISP	S0/0/1	209.165.201.2	255.255.255.252

Learning Objectives

Upon completion of this lab, you will be able to:

- Prepare the network
- Load routers with scripts
- Find and correct network errors
- Document the corrected network

Scenario

The routers, R1 and R2, at your company were configured by an inexperienced network engineer. Several errors in the configuration have resulted in connectivity issues. Your boss has asked you to troubleshoot and correct the configuration errors and document your work. Using your knowledge of DHCP, NAT, and standard testing methods, find and correct the errors. Make sure all clients have full connectivity. The ISP has been configured correctly.

Ensure that the network supports the following:

1. The router R2 should serve as the DHCP server for the 172.16.10.0/24 and 172.16.11.0/24 networks connected to R1.
2. All PCs connected to R1 should receive an IP address in the correct network via DHCP.
3. Traffic from the R1 LANs entering the Serial 0/0/0 interface on R2 and exiting the Serial 0/0/1 interface on R2 should receive NAT translation with a pool of addresses provided by the ISP.
4. The Inside Server should be reachable from outside networks using IP address 209.165.201.30, and to inside networks using IP address 172.16.20.254

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

Step 2: Clear all existing configurations on the routers.

Step 3: Import the configurations below.

R1

```
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 172.16.10.1 255.255.255.0
 ip helper-address 172.16.0.2
 no shutdown
!
interface FastEthernet0/1
 ip address 172.16.11.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.0.1 255.255.255.252
 clock rate 125000
 no shutdown
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
banner motd $AUTHORIZED ACCESS ONLY$
!
```

```
line con 0
password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 logging synchronous
 login
!
end
```

R2

```
hostname R2
!
enable secret class
!
ip dhcp excluded-address 172.16.10.1 172.16.10.3
ip dhcp excluded-address 172.16.11.1 172.16.11.3
!
ip dhcp pool R1_LAN10
 network 172.16.10.0 255.255.255.0
 dns-server 172.16.20.254
!
ip dhcp pool R1_LAN11
 network 172.16.11.0 255.255.255.0
 dns-server 172.16.20.254
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 172.16.20.1 255.255.255.0
 ip nat inside
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.0.2 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 ip address 209.165.201.1 255.255.255.252
 ip nat outside
 clock rate 125000
 no shutdown
!
router rip
 version 2
 network 172.16.0.0
 default-information originate
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 209.165.201.2
!
ip nat pool NAT_POOL 209.165.201.9 209.165.201.14 netmask 255.255.255.248
ip nat inside source list NAT_ACL pool NATPOOL overload
!
```

```
ip access-list standard NAT_ACL
  permit 172.16.10.0 0.0.0.255
!
banner motd $AUTHORIZED ACCESS ONLY$
!
line con 0
  password cisco
  logging synchronous
  login
line vty 0 4
  password cisco
  logging synchronous
  login
!
end
```

ISP

```
hostname ISP
!
enable secret class
!
interface Serial0/0/1
  ip address 209.165.201.2 255.255.255.252
  no shutdown
!
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
!
banner motd $AUTHORIZED ACCESS ONLY$
!
line con 0
  password cisco
  logging synchronous
  login
line vty 0 4
  password cisco
  logging synchronous
  login
!
end
```

Task 2: Find and Correct Network Errors

When the network is configured correctly:

- PC1 and PC2 should be able to receive IP addresses from the correct DHCP pool as evidenced by an ipconfig on the PCs. Additionally; a show ip dhcp bindings on R2 should show that both PCs have received IP addresses.
- Test pings from PC1 and PC2 to the ISP should receive NAT overload translation as evidenced by a show ip nat translations on R2.
- Test pings from the Inside Server to ISP should receive the static NAT translation indicated on the topology. Use the show ip nat translations command to verify this.
- A ping from the ISP to the global address of the Inside Server should be successful.

- Test pings from ISP to R1 should not receive NAT translation as evidenced by a `show ip nat translations` or a `debug ip nat` on R2.

Task 3: Document the Router Configurations

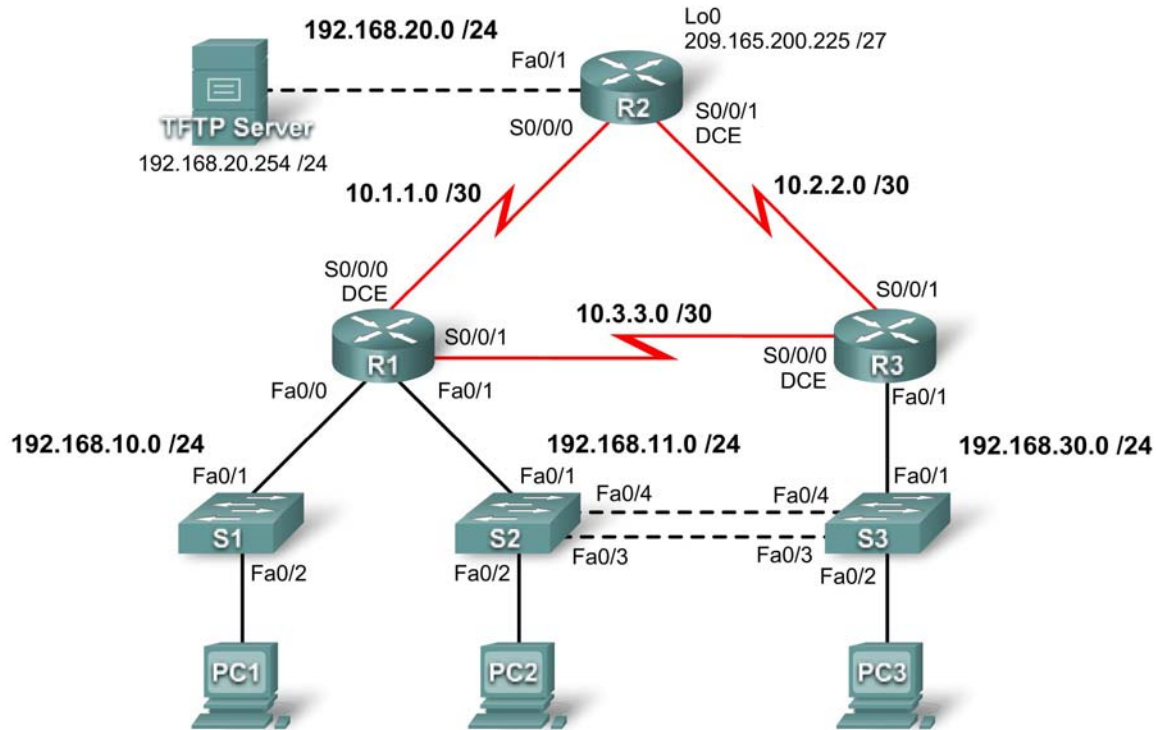
On each router, issue the **show run** command and capture the configurations.

Task 4: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks, such as the school LAN or to the Internet, reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 8.5.1: Troubleshooting Enterprise Networks 1

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.10.1	255.255.255.0	N/A
	Fa0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	Fa0/1	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	209.165.200.226
R3	Fa0/1	N/A	N/A	N/A
	Fa0/1.11	192.168.11.3	255.255.255.0	N/A
	Fa0/1.30	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.3.3.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
S1	VLAN10	DHCP	255.255.255.0	N/A
S2	VLAN11	192.168.11.2	255.255.255.0	N/A
S3	VLAN30	192.168.30.2	255.255.255.0	N/A

PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
TFTP Server	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Load the routers and switches with supplied scripts
- Find and correct all network errors
- Document the corrected network

Scenario

You have been asked to correct configuration errors in the company network. For this lab, do not use login or password protection on any console lines to prevent accidental lockout. Use **ciscoccna** for all passwords in this scenario.

Note: Because this lab is cumulative, you will be using all the knowledge and troubleshooting techniques that you have acquired from the previous material to successfully complete this lab.

Requirements

- S2 is the spanning-tree root for VLAN 11, and S3 is the spanning-tree root for VLAN 30.
- S3 is a VTP server with S2 as a client.
- The serial link between R1 and R2 is Frame Relay. Make sure that each router can ping their own Frame Relay interface.
- The serial link between R2 and R3 uses HDLC encapsulation.
- The serial link between R1 and R3 uses PPP.
- The serial link between R1 and R3 is authenticated using CHAP.
- R2 must have secure login procedures because it is the Internet edge router.
- All vty lines, except those belonging to R2, allow connections only from the subnets shown in the topology diagram, excluding the public address.

Hint:

R2# **telnet 10.1.1.1 /source-interface loopback 0**

Trying 10.1.1.1 ...

% Connection refused by remote host

- Source IP address spoofing should be prevented on all links that do not connect to other routers.
- Routing protocols must be secured. All RIP routers must use MD5 authentication.
- R3 must not be able to telnet to R2 through the directly connected serial link.
- R3 has access to both VLAN 11 and 30 via its Fast Ethernet port 0/0.
- The TFTP server should not get any traffic that has a source address outside the subnet. All devices have access to the TFTP server.
- All devices on the 192.168.10.0 subnet must be able to get their IP addresses from DHCP on R1. This includes S1.

- R1 must be accessible via SDM.
- All addresses shown in the diagram must be reachable from every device.

Task 1: Load Routers with the Supplied Scripts

```
!-----  
!  
!-----  
no service password-encryption  
!  
hostname R1  
!  
boot-start-marker  
boot-end-marker  
!  
security passwords min-length 6  
enable secret 5 ciscocna  
!  
ip cef  
!  
ip dhcp pool Access1  
    network 192.168.10.0 255.255.255.0  
    default-router 192.168.10.1  
!  
no ip domain lookup  
!  
username R3 password 0 ciscocna  
username ccna password 0 ciscocna  
!  
interface FastEthernet0/0  
    ip address 192.168.10.1 255.255.255.0  
    ip rip authentication mode md5  
    ip rip authentication key-chain RIP_KEY  
    no shutdown  
!  
interface FastEthernet0/1  
    ip address 192.168.11.1 255.255.255.0  
    ip rip authentication mode md5  
    ip rip authentication key-chain RIP_KEY  
    no shutdown  
!  
interface Serial0/0/0  
    ip address 10.1.1.1 255.255.255.252  
    ip rip authentication mode md5  
    ip rip authentication key-chain RIP_KEY  
    encapsulation frame-relay  
  
    clockrate 128000  
    frame-relay map ip 10.1.1.1 201  
    frame-relay map ip 10.1.1.2 201 broadcast  
    no frame-relay inverse-arp  
    no shutdown  
!  
interface Serial0/0/1
```

```
ip address 10.3.3.1 255.255.255.252
ip rip authentication mode md5
ip rip authentication key-chain RIP_KEY
encapsulation ppp
ppp authentication chap
no shutdown
!
!
router rip
version 2
passive-interface default
network 192.168.10.0
network 192.168.11.0
no auto-summary
!
ip classless
!
no ip http server
!
ip access-list standard Anti-spoofing
permit 192.168.10.0 0.0.0.255
deny any
ip access-list standard VTY
permit 10.0.0.0 0.255.255.255
permit 192.168.10.0 0.0.0.255
permit 192.168.11.0 0.0.0.255
permit 192.168.20.0 0.0.0.255
permit 192.168.30.0 0.0.0.255
!
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
access-class VTY in
login local
!
end
!-----
!                               R2
!-----
no service password-encryption
!
hostname R2
!
security passwords min-length 6
enable secret ciscocna
!
aaa new-model
!
aaa authentication login LOCAL_AUTH local
aaa session-id common
!
ip cef
!
no ip domain lookup
```

```
!  
key chain RIP_KEY  
  key 1  
    key-string cisco  
username ccna password 0 ciscoccna  
!  
interface Loopback0  
  description Simulated ISP Connection  
  ip address 209.165.200.245 255.255.255.224  
!  
interface FastEthernet0/0  
  ip address 192.168.20.1 255.255.255.0  
  ip access-group TFTP out  
  ip access-group Anti-spoofing in  
  ip nat outside  
  duplex auto  
  speed auto  
!  
interface FastEthernet0/1  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
!  
interface Serial0/0/0  
  ip address 10.1.1.2 255.255.255.0  
  ip nat inside  
  encapsulation frame-relay  
  no keepalive  
  frame-relay map ip 10.1.1.1 201 broadcast  
  no frame-relay inverse-arp  
!  
interface Serial0/0/1  
  ip address 10.2.2.1 255.255.255.0  
  ip access-group R3-telnet in  
  ip nat inside  
  ip rip authentication mode md5  
  ip rip authentication key-chain RIP_KEY  
  clockrate 128000  
!  
!  
router rip  
  version 2  
  passive-interface default  
  no passive-interface Serial0/0/0  
  no passive-interface Serial0/0/1  
  network 10.0.0.0  
  network 192.168.20.0  
  default-information originate  
  no auto-summary  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 209.165.200.226  
!  
no ip http server  
ip nat inside source list NAT interface FastEthernet0/0 overload
```

```
!  
ip access-list standard Anti-spoofing  
  permit 192.168.20.0 0.0.0.255  
  deny any  
ip access-list standard NAT  
  permit 10.0.0.0 0.255.255.255  
  permit 192.168.0.0 0.0.255.255  
!  
ip access-list extended R3-telnet  
  deny tcp host 10.2.2.2 host 10.2.2.1 eq telnet  
  deny tcp host 10.3.3.2 host 10.2.2.1 eq telnet  
  deny tcp host 192.168.11.3 host 10.2.2.1 eq telnet  
  deny tcp host 192.168.30.1 host 10.2.2.1 eq telnet  
  permit ip any any  
!  
ip access-list standard TFTP  
  permit 192.168.20.0 0.0.0.255  
!  
control-plane  
!  
line con 0  
  exec-timeout 0 0  
  logging synchronous  
line aux 0  
  exec-timeout 15 0  
  logging synchronous  
  login authentication local_auth  
  transport output telnet  
line vty 0 4  
  exec-timeout 15 0  
  logging synchronous  
  login authentication local_auth  
  transport input telnet  
!  
end  
!-----  
!  
! R3  
!-----  
no service password-encryption  
!  
hostname R3  
!  
security passwords min-length 6  
enable secret ciscocna  
!  
no aaa new-model  
!  
ip cef  
!  
no ip domain lookup  
!  
key chain RIP_KEY  
  key 1  
    key-string cisco  
username R1 password 0 ciscocna  
username ccna password 0 ciscocna
```

```
!  
interface FastEthernet0/1  
  no shutdown  
!  
interface FastEthernet0/1.11  
  encapsulation dot1Q 11  
  ip address 192.168.11.3 255.255.255.0  
  no snmp trap link-status  
!  
interface FastEthernet0/1.30  
  encapsulation dot1Q 30  
  ip address 192.168.30.1 255.255.255.0  
  ip access-group Anti-spoofing in  
  no snmp trap link-status  
!  
!  
interface Serial0/0/0  
  ip address 10.3.3.2 255.255.255.252  
  encapsulation ppp  
  clockrate 125000  
  ppp authentication chap  
!  
interface Serial0/0/1  
  ip address 10.2.2.2 255.255.255.252  
!  
router rip  
  version 2  
  passive-interface default  
  no passive-interface FastEthernet0/0.11  
  no passive-interface FastEthernet0/0.30  
  no passive-interface Serial0/0/0  
  no passive-interface Serial0/0/1  
  network 10.0.0.0  
  network 192.168.11.0  
  network 192.168.30.0  
  no auto-summary  
!  
ip classless  
!  
ip http server  
!  
ip access-list standard Anti-spoofing  
  permit 192.168.30.0 0.0.0.255  
  deny any  
ip access-list standard VTY  
  permit 10.0.0.0 0.255.255.255  
  permit 192.168.10.0 0.0.0.255  
  permit 192.168.11.0 0.0.0.255  
  permit 192.168.20.0 0.0.0.255  
  permit 192.168.30.0 0.0.0.255  
!  
control-plane  
!  
line con 0  
  exec-timeout 0 0  
  logging synchronous
```

```
line aux 0
  exec-timeout 15 0
  logging synchronous
line vty 0 4
  access-class VTY in
  exec-timeout 15 0
  logging synchronous
  login local
!
end
!-----
!                               S1
!-----
no service password-encryption
!
hostname S1
!
security passwords min-length 6
enable secret ciscocna
!
no aaa new-model
vtp domain CCNA_Troubleshooting
vtp mode transparent
vtp password ciscocna
ip subnet-zero
!
no ip domain-lookup
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 10
!
interface FastEthernet0/1
  switchport access vlan 10
  switchport mode access
!
interface FastEthernet0/2
  switchport access vlan 10
  switchport mode access
!
interface range FastEthernet0/3-24
!
interface GigabitEthernet0/1
  shutdown
!
interface GigabitEthernet0/2
  shutdown
!
interface Vlan1
  no ip address
  no ip route-cache
!
```

```
interface Vlan10
  ip address dhcp
  no ip route-cache
!
ip default-gateway 192.168.10.1
ip http server
!
control-plane
!
line con 0
  exec-timeout 0 0
  logging synchronous
line vty 0 4
  password ciscocna
  login
line vty 5 15
  no login
!
end
!-----
!                               S2
!-----
no service password-encryption
!
hostname S2
!
security passwords min-length 6
enable secret ciscocna
!
no aaa new-model
vtp domain CCNA_Troubleshooting
vtp mode transparent
vtp password ciscocna
ip subnet-zero
!
no ip domain-lookup
!
no file verify auto
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 11 priority 24576
spanning-tree vlan 30 priority 28672
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
  switchport access vlan 11
  switchport mode access
!
interface FastEthernet0/2
  switchport access vlan 11
  switchport mode access
!
interface FastEthernet0/3
  switchport trunk native vlan 99
```

```
switchport trunk allowed vlan 11,30
switchport mode trunk
!
interface FastEthernet0/4
switchport trunk native vlan 99
switchport trunk allowed vlan 11,30
switchport mode trunk
!
interface range FastEthernet0/5-24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
no ip address
no ip route-cache
!
interface Vlan11
ip address 192.168.11.2 255.255.255.0
no ip route-cache
!
ip http server
!
control-plane
!
line con 0
exec-timeout 0 0
logging synchronous
line vty 0 4
password ciscocna
login
line vty 5 15
no login
!
end
!-----
!                               S3
!-----
no service password-encryption
!
hostname S3
!
security passwords min-length 6
enable secret ciscocna
!
no aaa new-model
vtp domain CCNA_troubleshooting
vtp mode server
vtp password ciscocna
ip subnet-zero
!
no ip domain-lookup
```



```
!  
no file verify auto  
!  
spanning-tree mode rapid-pvst  
spanning-tree extend system-id  
spanning-tree vlan 11 priority 28672  
spanning-tree vlan 30 priority 24576  
!  
vlan internal allocation policy ascending  
!  
!  
interface FastEthernet0/1  
    switchport trunk allowed vlan 30  
    switchport mode trunk  
!  
interface FastEthernet0/2  
    switchport access vlan 30  
    switchport mode access  
!  
interface FastEthernet0/3  
    switchport trunk native vlan 99  
    switchport trunk allowed vlan 11,30  
    switchport mode trunk  
!  
interface FastEthernet0/4  
    switchport trunk native vlan 99  
    switchport trunk allowed vlan 11,30  
    switchport mode trunk  
!  
interface range FastEthernet0/5-24  
    shutdown  
!  
interface GigabitEthernet0/1  
    shutdown  
!  
interface GigabitEthernet0/2  
    shutdown  
!  
interface Vlan1  
    no ip address  
    no ip route-cache  
!  
interface Vlan30  
    ip address 192.168.30.2 255.255.255.0  
    no ip route-cache  
!  
ip default-gateway 192.168.30.1  
ip http server  
!  
control-plane  
!  
line con 0  
    exec-timeout 5 0  
    logging synchronous  
line vty 0 4  
    password ciscocna
```

```
login
line vty 5 15
  no login
!
end
```

Task 2: Find and Correct All Network Errors

Task 3: Verify that Requirements Are Fully Met

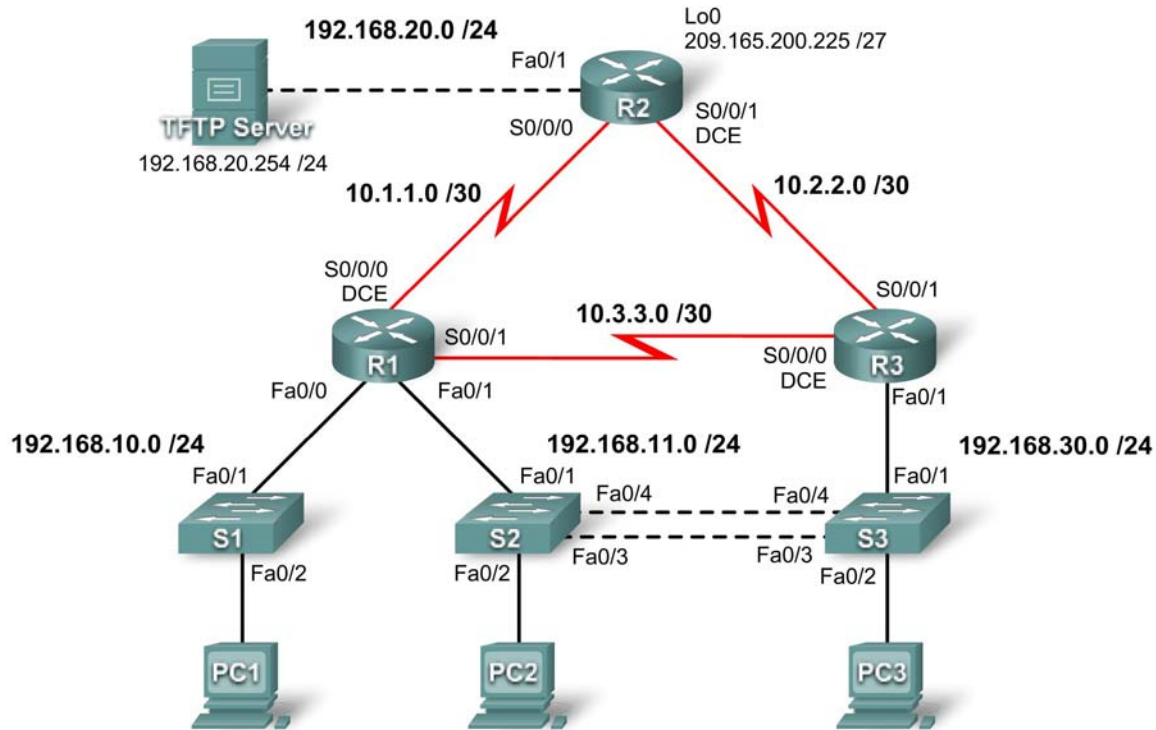
Task 4: Document the Corrected Network

Task 5: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 8.5.2: Troubleshooting Enterprise Networks 2

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.10.1	255.255.255.0	N/A
	Fa0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	Fa0/1	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	209.165.200.226
R3	Fa0/1	N/A	N/A	N/A
	Fa0/1.11	192.168.11.3	255.255.255.0	N/A
	Fa0/1.30	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.3.3.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
S1	VLAN10	DHCP		N/A
S2	VLAN11	192.168.11.2	255.255.255.0	N/A
S3	VLAN30	192.168.30.2	255.255.255.0	N/A
PC1	NIC	DHCP		
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1

PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
TFTP Server	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Load the routers and switches with supplied scripts
- Find and correct all network errors
- Document the corrected network

Scenario

For this lab, do not use login or password protection on any console lines to prevent accidental lockout. Use **ciscoccna** for all passwords in this lab.

Note: Because this lab is cumulative, you will be using all the knowledge and troubleshooting techniques that you have acquired from the previous material to successfully complete this lab.

Requirements

- S2 is the spanning-tree root for VLAN 11, and S3 is the spanning-tree root for VLAN 30.
- S3 is a VTP server with S2 as a client.
- The serial link between R1 and R2 is Frame Relay.
- The serial link between R2 and R3 uses HDLC encapsulation.
- The serial link between R1 and R3 is authenticated using CHAP.
- R2 must have secure login procedures because it is the Internet edge router.
- All vty lines, except those belonging to R2, allow connections only from the subnets shown in the topology diagram, excluding the public address.
- Source IP address spoofing should be prevented on all links that do not connect to other routers.
- Routing protocols must be used securely. EIGRP is used in this scenario.
- R3 must not be able to telnet to R2 through the directly connected serial link.
- R3 has access to both VLAN 11 and 30 via its Fast Ethernet port 0/1.
- The TFTP server should not get any traffic that has a source address outside the subnet. All devices have access to the TFTP server.
- All devices on the 192.168.10.0 subnet must be able to get their IP addresses from DHCP on R1. This includes S1.
- All addresses shown in diagram must be reachable from every device.

Task 1: Load Routers with the Supplied Scripts

```
!-----
!  
!                               R1  
!-----
no service password-encryption
!  
hostname R1  
!
```

```
boot-start-marker
boot-end-marker
!
security passwords min-length 6
enable secret ciscocna
!
ip cef
!
ip dhcp pool Access1
    network 192.168.10.0 255.255.255.0
    default-router 192.168.10.1
!
no ip domain lookup
frame-relay switching
!
username R2 password ciscocna
username ccna password ciscocna
!
interface FastEthernet0/0
    ip address 192.168.10.1 255.255.255.0
    ip access-group Anti-spoofing out
    duplex auto
    speed auto
    no shutdown
!
interface FastEthernet0/1
    ip address 192.168.11.1 255.255.255.0
    duplex auto
    speed auto
    no shutdown
!
interface Serial0/0/0
    ip address 10.1.1.1 255.255.255.252
    encapsulation frame-relay
    no keepalive
    clockrate 128000
    frame-relay map ip 10.1.1.1 201
    frame-relay map ip 10.1.1.2 201 broadcast
    no frame-relay inverse-arp
    frame-relay intf-type dce
    no shutdown
!
interface Serial0/0/1
    ip address 10.3.3.1 255.255.255.0
    encapsulation ppp
    ppp authentication chap
    no shutdown
!
!
router eigrp 10
    passive-interface default
    no passive-interface FastEthernet0/0
    no passive-interface FastEthernet0/1
    no passive-interface Serial0/0/0
    no passive-interface Serial0/0/1
    network 10.1.1.0 0.0.0.255
```

```
network 10.2.2.0 0.0.0.255
network 192.168.10.0 0.0.0.255
network 192.168.11.0 0.0.0.255
no auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
ip http server
!
ip access-list standard Anti-spoofing
  permit 192.168.10.0 0.0.0.255
  deny any
ip access-list standard VTY
  permit 10.0.0.0 0.255.255.255
  permit 192.168.10.0 0.0.0.255
  permit 192.168.11.0 0.0.0.255
  permit 192.168.20.0 0.0.0.255
  permit 192.168.30.0 0.0.0.255
!
line con 0
  exec-timeout 5 0
  logging synchronous
line aux 0
line vty 0 4
  access-class VTY in
  login local
!
end
!-----
!                               R2
!-----
no service password-encryption
!
hostname R2
!
security passwords min-length 6
enable secret ciscocna
!
aaa new-model
!
aaa authentication login local_auth local
aaa session-id common
!
ip cef
!
no ip domain lookup
!
username ccna password 0 ciscocna
!
interface Loopback0
  ip address 209.165.200.225 255.255.255.224
  ip access-group private in
!
interface FastEthernet0/1
  ip address 192.168.20.1 255.255.255.0
  ip access-group TFTP out
```

```
ip access-group Anti-spoofing in
ip nat outside
no shutdown
!
!
interface Serial0/0/0
ip address 10.1.1.2 255.255.255.252
ip nat inside
encapsulation frame-relay
no keepalive
frame-relay map ip 10.1.1.1 201 broadcast
frame-relay map ip 10.1.1.2 201
no frame-relay inverse-arp
no shutdown
!
interface Serial0/0/1
ip address 10.2.2.1 255.255.255.252
ip nat inside
clockrate 128000
no shutdown
!
!
router eigrp 100
passive-interface default
no passive-interface FastEthernet0/1
no passive-interface Serial0/0/0
no passive-interface Serial0/0/1
no passive interface lo0
network 10.1.1.0 0.0.0.3
network 10.2.2.0 0.0.0.3
network 192.168.20.0 0.0.0.255
network 209.165.200.0 0.0.0.7
no auto-summary
!
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
no ip http server
ip nat inside source list NAT interface FastEthernet0/0 overload
!
ip access-list standard Anti-spoofing
permit 192.168.20.0 0.0.0.255
deny any
ip access-list standard NAT
permit 10.0.0.0 0.255.255.255
permit 192.168.0.0 0.0.255.255
ip access-list standard private
deny 127.0.0.1
deny 10.0.0.0 0.255.255.255
deny 172.16.0.0 0.15.255.255
deny 192.168.0.0 0.0.255.255
permit any
!
ip access-list extended R3-telnet
deny tcp host 10.2.2.2 host 10.2.2.1 eq telnet
deny tcp host 10.3.3.2 host 10.2.2.1 eq telnet
deny tcp host 192.168.11.3 host 10.2.2.1 eq telnet
```

```
deny    tcp host 192.168.30.1 host 10.2.2.1 eq telnet

!
ip access-list standard TFTP
 permit 192.168.20.0 0.0.0.255
!
control-plane
!
line con 0
 exec-timeout 5 0
 logging synchronous
line aux 0
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport output telnet
line vty 0 4
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport input telnet
!
end
!-----
!                               R3
!-----
no service password-encryption
!
hostname R3
!
security passwords min-length 6
!
no aaa new-model
!
ip cef
!
no ip domain lookup
!
username R1 password ciscoccna
username ccna password  ciscoccna
!
interface FastEthernet0/1
 no shutdown
!
interface FastEthernet0/1.11
 encapsulation dot1Q 11
 ip address 192.168.11.3 255.255.255.0
 no snmp trap link-status
!
interface FastEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip access-group Anti-Spoofin in
 no shutdown
!
!
```



```
interface Serial0/0/0
 ip address 10.3.3.2 255.255.255.252
 encapsulation ppp
 ppp authentication pap
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 no shutdown
!
router eigrp 10
 network 10.3.3.0 0.0.0.3
 network 10.2.2.0 0.0.0.3
 network 192.168.11.0 0.0.0.255
 network 192.168.30.0 0.0.0.255
 no auto-summary
!
ip classless
!
ip http server
!
ip access-list standard Anti-spoofing
 permit 192.168.30.0 0.0.0.255
 deny any
ip access-list standard VTY
 permit 10.0.0.0 0.255.255.255
 permit 192.168.10.0 0.0.0.255
 permit 192.168.11.0 0.0.0.255
 permit 192.168.20.0 0.0.0.255
 permit 192.168.30.0 0.0.0.255
!
!
line con 0
 exec-timeout 5 0
 logging synchronous
line aux 0
 exec-timeout 15 0
 logging synchronous
line vty 0 4
 access-class VTY out
 exec-timeout 15 0
 logging synchronous
 login local
!
end
!-----
!                               S1
!-----
no service password-encryption
!
hostname S1
!
security passwords min-length 6
enable secret ciscoccna
!
no aaa new-model
vtp domain CCNA_Troubleshooting
```

```
vtp mode transparent
vtp password ciscocna
ip subnet-zero
!
no ip domain-lookup
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 10
!
interface FastEthernet0/1
    switchport access vlan 10
    switchport mode access
!
interface FastEthernet0/2
    switchport access vlan 10
    switchport mode access
!
interface range FastEthernet0/3-24
!
interface GigabitEthernet0/1
    shutdown
!
interface GigabitEthernet0/2
    shutdown
!
interface Vlan1
    no ip address
    no ip route-cache
!
interface Vlan10
    ip address dhcp
    no ip route-cache
!
ip default-gateway 192.168.10.1
ip http server
!
line con 0
    exec-timeout 5 0
    logging synchronous
line vty 0 4
    password ciscocna
    login
line vty 5 15
    no login
!
end
!-----
!                               S2
!-----
no service pad
service timestamps debug uptime
```

```
service timestamps log uptime
no service password-encryption
!
hostname S2
!
security passwords min-length 6
enable secret ciscocna
!
no aaa new-model
vtp domain CCNA_Troubleshooting
vtp mode Client
vtp password ciscocna
ip subnet-zero
!
no ip domain-lookup
!
no file verify auto
!
spanning-tree mode mst
spanning-tree extend system-id
spanning-tree vlan 30 priority 4096
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
    switchport access vlan 11
    switchport mode access
!
interface FastEthernet0/2
    switchport access vlan 11
    switchport mode access
!
interface FastEthernet0/3
    switchport trunk allowed vlan 11,30
    switchport mode trunk
!
interface FastEthernet0/4
    switchport trunk allowed vlan 11,30
    switchport mode trunk
!
interface range FastEthernet0/5-24
    shutdown
!
interface GigabitEthernet0/1
    shutdown
!
interface GigabitEthernet0/2
    shutdown
!
interface Vlan1
    no ip address
    no ip route-cache
!
interface Vlan11
    ip address 192.168.11.2 255.255.255.0
    no ip route-cache
```

```
!  
ip http server  
!  
control-plane  
!  
line con 0  
    exec-timeout 5 0  
    logging synchronous  
line vty 0 4  
    password ciscocna  
    login  
line vty 5 15  
    no login  
!  
end  
!-----  
!                S3  
!-----  
no service password-encryption  
!  
hostname S3  
!  
security passwords min-length 6  
enable secret ciscocna  
!  
no aaa new-model  
vtp domain CCNA_Troubleshooting  
vtp mode Server  
vtp password ciscocna  
ip subnet-zero  
!  
no ip domain-lookup  
!  
no file verify auto  
!  
spanning-tree mode rapid-pvst  
spanning-tree extend system-id  
spanning-tree vlan 11 priority 4096  
vlan internal allocation policy ascending  
!  
Vlan 11,30  
!  
interface FastEthernet0/1  
    switchport trunk allowed vlan 11,30  
    switchport mode trunk  
!  
interface FastEthernet0/2  
    switchport access vlan 30  
    switchport mode access  
!  
interface FastEthernet0/3  
  
    switchport trunk allowed vlan 11,30  
    switchport mode trunk  
!  
interface FastEthernet0/4
```

```
switchport trunk allowed vlan 11,30
switchport mode trunk
!
interface range FastEthernet0/5-24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
no ip address
no ip route-cache
!
interface Vlan30
ip address 192.168.30.2 255.255.255.0
no ip route-cache
!
ip default-gateway 192.168.30.1
ip http server
!
line con 0
exec-timeout 5 0
logging synchronous
line vty 0 4
password ciscocena
login
line vty 5 15
no login
!
end
```

Task 2: Find and Correct All Network Errors

Task 3: Verify that Requirements Are Fully Met

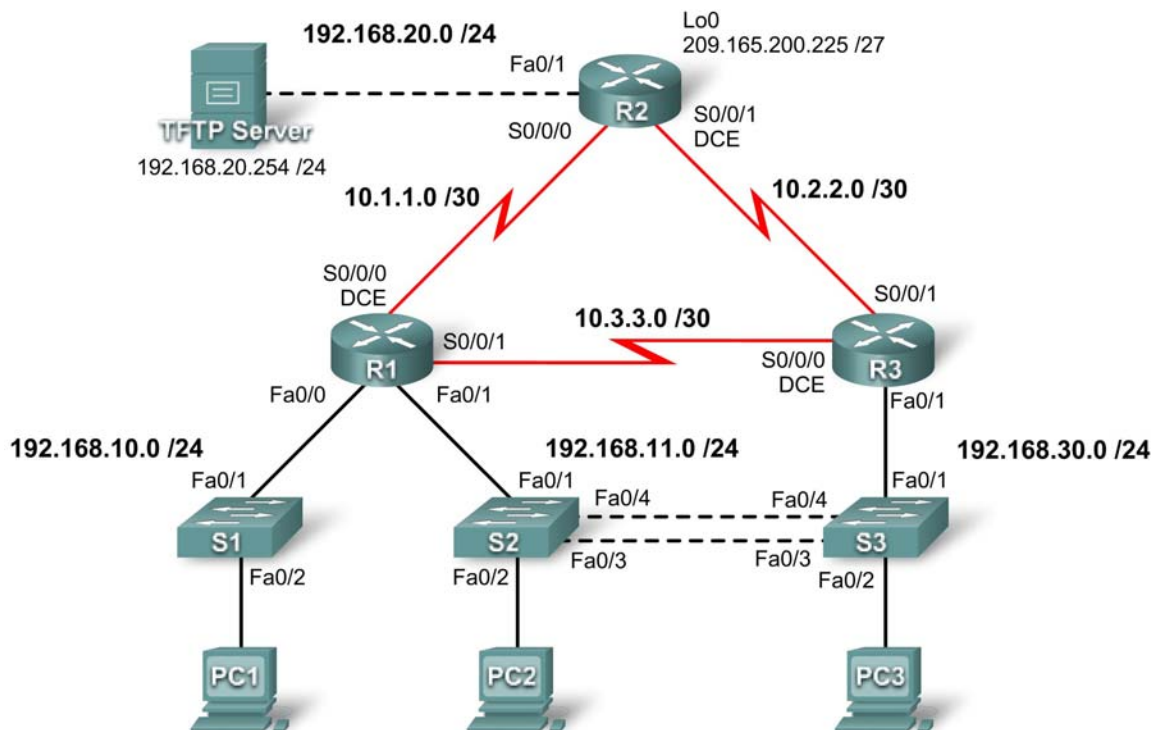
Task 4: Document the Corrected Network

Task 5: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Lab 8.5.3: Troubleshooting Enterprise Networks 3

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.10.1	255.255.255.0	N/A
	Fa0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	Fa0/1	192.168.20.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	209.165.200.226
R3	Fa0/1	N/A	N/A	N/A
	Fa0/1.11	192.168.11.3	255.255.255.0	N/A
	Fa0/1.30	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.3.3.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
S1	VLAN10	DHCP	255.255.255.0	N/A
S2	VLAN11	192.168.11.2	255.255.255.0	N/A
S3	VLAN30	192.168.30.2	255.255.255.0	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1

PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
TFTP Server	NIC	192.168.20.254	255.255.255.0	192.168.20.1

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Load the routers and switches with supplied scripts
- Find and correct all network errors
- Document the corrected network

Scenario

For this lab do not use login or password protection on any console lines to prevent accidental lockout. Use **ciscoccna** for all passwords in this scenario.

Note: Because this lab is cumulative, you will be using all the knowledge and troubleshooting techniques that you have acquired from the previous material to successfully complete this lab.

Requirements

- S2 is the spanning-tree root for VLAN 11, and S3 is the spanning-tree root for VLAN 30.
- S3 is a VTP server with S2 as a client.
- The serial link between R1 and R2 is Frame Relay.
- The serial link between R2 and R3 uses HDLC encapsulation.
- The serial link between R1 and R3 is authenticated using CHAP.
- R2 must have secure login procedures because it is the Internet edge router.
- All vty lines, except those belonging to R2, allow connections only from the subnets shown in the topology diagram, excluding the public address.
- Source IP address spoofing should be prevented on all links that do not connect to other routers.
- Routing protocols must be used securely. OSPF is used in this scenario.
- R3 must not be able to telnet to R2 through the directly connected serial link.
- R3 has access to both VLAN 11 and 30 via its Fast Ethernet port 0/1.
- The TFTP server should not get any traffic that has a source address outside the subnet. All devices have access to the TFTP server.
- All devices on the 192.168.10.0 subnet must be able to get their IP addresses from DHCP on R1. This includes S1.
- All addresses shown in diagram must be reachable from every device.

Task 1: Load Routers with the Supplied Scripts

```
!-----
!  
!                               R1  
!-----
no service password-encryption
!  
hostname R1  
!
```

```
boot-start-marker
boot-end-marker
!
security passwords min-length 6
enable secret ciscocna
!
ip cef
!
ip dhcp pool Access1
    network 192.168.11.0 255.255.255.0
    default-router 192.168.10.1
!
no ip domain lookup
!
ip dhcp excluded-address 192.168.10.2 192.168.10.254
!
frame-relay switching
!
username R3 password 0 ciscocna
username ccna password 0 ciscocna
!
interface FastEthernet0/0
    ip address 192.168.10.1 255.255.255.0
    duplex auto
    speed auto
    no shutdown
!
interface FastEthernet0/1
    ip address 192.168.11.1 255.255.255.0
    duplex auto
    speed auto
no shutdown
!
interface Serial0/0/0
    ip address 10.1.1.1 255.255.255.252
    encapsulation frame-relay
    no keepalive
    clockrate 128000
    frame-relay map ip 10.1.1.1 201
    frame-relay map ip 10.1.1.2 201 broadcast
    no frame-relay inverse-arp
    frame-relay intf-type dce
    no shutdown
!
interface Serial0/0/1
    ip address 10.3.3.1 255.255.255.252
    encapsulation ppp
    ppp authentication chap
    no shutdown
!
interface Serial0/1/0
    no ip address
    shutdown
    clockrate 2000000
!
interface Serial0/1/1
```



```
no ip address
shutdown
!
router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet0/0
 network 10.1.1.0 0.0.0.255 area 0
 network 10.2.2.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
!
ip http server
!
ip access-list standard Anti-spoofing
 permit 192.168.10.0 0.0.0.255
 deny any
ip access-list standard VTY
 permit 10.0.0.0 0.255.255.255
 permit 192.168.10.0 0.0.0.255
 permit 192.168.11.0 0.0.0.255
 permit 192.168.20.0 0.0.0.255
 permit 192.168.30.0 0.0.0.255
!
line con 0
 exec-timeout 5 0
 logging synchronous
line aux 0
line vty 0 4
 access-class VTY in
 login local
!
end
!-----
!                               R2
!-----
no service password-encryption
!
hostname R2
!
security passwords min-length 6
enable secret ciscocna
!
aaa new-model
!
aaa authentication login local_auth local
aaa session-id common
!
ip cef
!
no ip domain lookup
!
username ccna password 0 ciscocna
!
interface Loopback0
 ip address 209.165.200.245 255.255.255.224
 ip access-group private in
```

```
!  
interface FastEthernet0/1  
  ip address 192.168.20.1 255.255.255.0  
  ip access-group TFTP out  
  ip access-group Anti-spoofing in  
  ip nat inside  
  duplex auto  
  speed auto  
!  
!  
interface Serial0/0/0  
  ip address 10.1.1.2 255.255.255.252  
  ip nat outside  
  encapsulation frame-relay  
  no keepalive  
  frame-relay map ip 10.1.1.1 201 broadcast  
  frame-relay map ip 10.1.1.2 201  
  no frame-relay inverse-arp  
!  
interface Serial0/0/1  
  ip address 10.2.2.1 255.255.255.252  
  ip access-group R3-telnet in  
  ip nat outside  
!  
!  
router ospf 1  
  passive-interface FastEthernet0/1  
  network 10.1.1.0 0.0.0.3 area 0  
  network 10.2.2.0 0.0.0.3 area 0  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 209.165.200.226  
!  
no ip http server  
ip nat inside source list nat interface FastEthernet0/0  
!  
ip access-list standard Anti-spoofing  
  permit 192.168.20.0 0.0.0.255  
  deny any  
ip access-list standard NAT  
  permit 10.0.0.0 0.255.255.255  
  permit 192.168.0.0 0.0.255.255  
ip access-list standard private  
  deny 127.0.0.1  
  deny 10.0.0.0 0.255.255.255  
  deny 172.0.0.0 0.31.255.255  
  deny 192.168.0.0 0.0.255.255  
  permit any  
!  
ip access-list extended R3-telnet  
  deny tcp host 10.2.2.2 host 10.2.2.1 eq telnet  
  deny tcp host 10.3.3.2 host 10.2.2.1 eq telnet  
  deny tcp host 192.168.11.3 host 10.2.2.1 eq telnet  
  deny tcp host 192.168.30.1 host 10.2.2.1 eq telnet  
  permit ip any any  
!
```

```
ip access-list standard TFTP
 permit 192.168.20.0 0.0.0.255
!
line con 0
 exec-timeout 5 0
 logging synchronous
line aux 0
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport output telnet
line vty 0 4
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport input telnet
!
end
!-----
!                               R3
!-----
no service password-encryption
!
hostname R3
!
security passwords min-length 6
enable secret ciscocna
!
no aaa new-model
!
ip cef
!
no ip domain lookup
!
username R1 password ciscocna
username ccna password ciscocna
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 no shutdown
!
interface FastEthernet0/1.11
 encapsulation dot1Q 12
ip address 192.168.11.3 255.255.255.0
 no snmp trap link-status
!
interface FastEthernet0/1.30
 encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.0
ip access-group Anti-spoofing in
!
!
interface Serial0/0/0
ip address 10.3.3.2 255.255.255.252
```

```
encapsulation ppp
clockrate 125000
ppp authentication chap
no shutdown
!
interface Serial0/0/1
ip address 10.2.2.2 255.255.255.252
encapsulation lapb
no shutdown
!
router ospf 1
passive-interface FastEthernet0/1.30
network 10.2.2.0 0.0.0.3 area 1
network 10.3.3.0 0.0.0.3 area 1
network 192.168.11.0 0.0.0.255 area 1
network 192.168.30.0 0.0.0.255 area 1
!
ip classless
!
ip http server
!
ip access-list standard Anti-spoofing
permit 192.168.30.0 0.0.0.255
deny any
ip access-list standard VTY
permit 10.0.0.0 0.255.255.255
permit 192.168.10.0 0.0.0.255
permit 192.168.11.0 0.0.0.255
permit 192.168.20.0 0.0.0.255
permit 192.168.30.0 0.0.0.255
!
line con 0
exec-timeout 5 0
logging synchronous
line aux 0
exec-timeout 15 0
logging synchronous
line vty 0 4
access-class VTY in
exec-timeout 15 0
logging synchronous
login local
!
end
!-----
!                               S1
!-----
no service password-encryption
!
hostname S1
!
security passwords min-length 6
enable secret ciscocna
!
no aaa new-model
vtp domain CCNA_Troubleshooting
```

```
vtp mode transparent
vtp password ciscocna
ip subnet-zero
!
no ip domain-lookup
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 10
!
interface FastEthernet0/1
    switchport access vlan 10
    switchport mode access
!
interface FastEthernet0/2
    switchport access vlan 10
    switchport mode access
!
interface range FastEthernet0/3-24
!
interface GigabitEthernet0/1
    shutdown
!
interface GigabitEthernet0/2
    shutdown
!
interface Vlan1
    no ip address
    no ip route-cache
!
interface Vlan10
    ip address dhcp
    no ip route-cache
!
ip default-gateway 192.168.10.1
ip http server
!
line con 0
    exec-timeout 5 0
    logging synchronous
line vty 0 4
    password ciscocna
    login
line vty 5 15
    no login
!
end
!-----
!                               S2
!-----
no service pad
service timestamps debug uptime
```

```
service timestamps log uptime
no service password-encryption
!
hostname S2
!
security passwords min-length 6
enable secret ciscocna
!
no aaa new-model
vtp domain CCNA_Troubleshooting
vtp mode client
vtp password ciscocna
ip subnet-zero
!
no ip domain-lookup
!
no file verify auto
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 11 priority 24576
spanning-tree vlan 30 priority 28672
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
    switchport access vlan 11
    switchport mode access
!
interface FastEthernet0/2
    switchport access vlan 11
    switchport mode access
!
interface FastEthernet0/3
    switchport trunk allowed vlan 11,30
    switchport mode trunk
!
interface FastEthernet0/4
    switchport trunk allowed vlan 11,30
    switchport mode trunk
!
interface range FastEthernet0/5-24
    shutdown
!
interface GigabitEthernet0/1
    shutdown
!
interface GigabitEthernet0/2
    shutdown
!
interface Vlan1
    no ip address
    no ip route-cache
!
interface Vlan11
    ip address 192.168.11.2 255.255.255.0
```

```
no ip route-cache
!
ip http server
!
line con 0
  exec-timeout 5 0
  logging synchronous
line vty 0 4
  password ciscocna
  login
line vty 5 15
  no login
!
end
!-----
!                               S3
!-----
no service password-encryption
!
hostname S3
!
security passwords min-length 6
enable secret ciscocna
!
no aaa new-model
vtp domain CCNA_Troubleshooting
vtp mode Server
vtp password ciscocna
ip subnet-zero
!
no ip domain-lookup
!
no file verify auto
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 11 priority 28672
spanning-tree vlan 30 priority 24576
!
vlan internal allocation policy ascending
!
vlan 30
!
interface FastEthernet0/1
  switchport trunk allowed vlan 11
  switchport mode trunk
!
interface FastEthernet0/2
  switchport access vlan 30
  switchport mode access
!
interface FastEthernet0/3
  switchport trunk native vlan 99
  switchport trunk allowed vlan 11,30
  switchport mode trunk
!
```

```
interface FastEthernet0/4
  switchport trunk native vlan 99
  switchport trunk allowed vlan 11,30
  switchport mode trunk
!
interface range FastEthernet0/5-24
  shutdown
!
interface GigabitEthernet0/1
  shutdown
!
interface GigabitEthernet0/2
  shutdown
!
interface Vlan1
  no ip address
  no ip route-cache
!
interface Vlan30
  ip address 192.168.30.2 255.255.255.0
  no ip route-cache
!
ip default-gateway 192.168.30.1
ip http server
!
line con 0
  exec-timeout 5 0
  logging synchronous
line vty 0 4
  password ciscoccna
  login
line vty 5 15
  no login
!
end
```

Task 2: Find and Correct All Network Errors

Task 3: Verify that Requirements Are Fully Met

Because time constraints prevent troubleshooting a problem on each topic, only a select number of topics have problems. However, to reinforce and strengthen troubleshooting skills, you should verify that each requirement is met. To do this, present an example of each requirement (for example a **show** or **debug** command).

Task 4: Document the Corrected Network

Task 4: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.